IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application for:
Avaya Technology Corp.

Art Unit: 2155

First Named Inventor: CHAN et al.

Examiner: Wang, Liangche

Appln. No.: 10/622,982

Confirmation No.: 2989

Filing Date: July 17, 2003

For: "Method and Apparatus For Restriction of Message Distribution For Security"

* * *

APPELLANTS' BRIEF
(37 CFR § 41.37)

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants hereby appeal to the Board of Appeals in response to the Notice of Panel Decision from Pre-Appeal Brief Review of May 24, 2007. The fee set forth in 37 CFR § 41.20(b) has been previously submitted in connection with the Request for Pre-Appeal Brief Request for Review. Although Appellants believe that no additional fees are due at this time, authorization to charge any necessary fees to Deposit Account No. 19-1970 is hereby given.

A single copy of this Appeal Brief is being submitted pursuant to MPEP § 1205.02.

(I) REAL PARTY IN INTEREST

All right, title, and interest in this application has been assigned by the inventors, Kevin Chan, Neil Hepworth, and Stephane C. Laveau, to Avaya Technology Corp. This Assignment is recorded at Reel/Frame 014306/0146.

(II) RELATED APPEALS AND INTERFERENCES

There are no related appeals, interferences or judicial proceedings known to Appellants, or the Appellants' legal representative which may be related to, directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

(III) STATUS OF CLAIMS

Claims 1-49 are pending in the application. Claims 32-35 have been withdrawn from consideration. Accordingly, Claims 1-31 and 36-49 are being appealed.

Claims 1, 3, 5-8, 10-11, 13-17, 19, 21-24, 26-27, 29-31, 36, 37, 39, 41-44, 46-47, and 49 stand rejected under 35 U.S.C.§102(e).

Claims 2, 4, 9, 12, 18, 20, 25, 28, 38, 40, 45, and 48 stand rejected under 35 U.S.C.§103(a).

The Claims at issue (*i.e.*, Claims 1-31 and 36-49) are set forth in the CLAIMS APPENDIX.

(IV) STATUS OF AMENDMENTS

An amendment was filed on April 4, 2007, subsequent to the Examiner's Final Office Action dated February 6, 2007. That amendment was denied entry by the Examiner in an Advisory Action dated April 18, 2007.

(V) SUMMARY OF CLAIMED SUBJECT MATTER

The currently pending Independent Claims 1, 16, and 36, recited in the Claims Appendix hereto, are directed to methods and a server for processing an electronic message (*See* Specification page 1, lines 5-7; page 4, lines 4-5; page 5, lines 7-8; and Fig. 1, elements 14a and 14b).

One embodiment, which is the subject of Independent Claim 1, is directed to a method for processing an electronic message, comprising:

receiving a message from a sender (*See* Specification page 4, line 6; page 20, lines 22-23; and Fig. 5, step 404), the message comprising **(I)** at least one recipient to receive the message (*See* Specification page 4, line 6; page 12, lines 16-20; and Fig. 4, step 308) and including at least one of **(a)** a restriction identifier, the restriction identifier identifying a subset of recipients from among a set of possible recipients (*See* Specification page 4, lines 7-8; page 12 and line 22 through page 13, line 13) and **(b)** an access restriction indicating a subset of points of access from among a set of points of access to access the message (*See* Specification page 3, line 23 through page 4, line 2; page 14, lines 9-13; and Fig. 6, step 504);

determining whether each identified at least one recipient is within the subset of recipients corresponding to the restriction identifier (*See* Specification page 4, lines 9-10; page 14, lines 1-2; and Fig. 5, step 412); and wherein at least one of the following steps is performed:

(i) when the message comprises the restriction identifier and an identified at least one recipient is not within the subset of recipients, at least one of **(A)** not providing access to the message to the identified at least one recipient who is not in the subset of recipients (*See* Specification page 4, lines 11-13; page 14, lines 2-3; and Fig. 5, step 412) and **(B)** notifying the sender that an identified at least one recipient is not within the subset of recipients (*See* Specification page 4, lines 13-14; page 14, lines 3-4; and Fig. 5, step 420); and

(ii) when the message comprises the access restriction and an identified at least one recipient attempts to access the message from a point of access not within the subset of points of access, not providing access to the message to the identified at least one recipient whose point of access is not within the subset of points of access (*See* Specification page 14, lines 16-17 and Fig. 6, step 516). [Bold identifiers added]

A related embodiment, which is the subject of Independent Claim 16, is directed toward a method for processing an electronic message, comprising:

receiving at least part of a message inputted by a user (*See* Specification page 4, line 6; page 13, lines 22-23; and Fig. 5, step 404), the at least part of a message comprising at least one recipient to receive the message (*See* Specification page 5, lines 9-10; page 12, lines 16-20; and Fig. 4, step 308);

receiving, from the user, a restriction identifier for the at least part of a message, the restriction identifier identifying a subset of recipients from among a set of possible recipients (*See* Specification page 5, lines 11-13; page 12, line 22 through page 13, line 13); and

when a restriction identifier is received, tagging the message with the restriction identifier (*See* Specification page 5, lines 14-15; page 10, lines 18-23, and Fig. 4, step 320).

Another embodiment, which is the subject of Independent Claim 36, is directed toward a server for processing an electronic message, comprising:

an input operable to receive at least part of a message inputted by a user (*See* Specification page 4, line 6; page 13, lines 22-23; and Fig. 5, step 404), the at least part of a message comprising at least one recipient to receive the message (*See* Specification page 5, lines 9-10; page 12, lines 16-20; and Fig. 4, step 308), and a restriction identifier for the at least part of a message, the restriction identifier identifying a subset of recipients from among a set of possible recipients (*See* Specification page 5, lines 11-13; page 12, line 22 through page 13, line 13); and

when a restriction identifier is received, a processor operable to tag the message with the restriction identifier (*See* Specification page 5, lines 11-13; page 12, line 22 through page 13, line 13).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 12, 28, and 48 are unpatentable under 35 U.S.C.§103(a) over U.S. Patent No. 6,480,885 [hereinafter "Olivier"] in view of U.S. Patent No. 5,619,648 [hereinafter "Canale"].

Whether Claims 1, 3, 5-8, 10-11, 13-17, 19, 21-24, 26-27, 29-31, 36, 37, 39, 41-44, 46-47, and 49 are anticipated under 35 U.S.C.§102(e) by Olivier.

Whether Claims 9, 25, and 45 are unpatentable under 35 U.S.C.§103(a) over Olivier in view of U.S. Patent No. 6,654,779 [hereinafter "Tsuei"].

(VII) ARGUMENT

1. Rejection of Claims 12, 28, and 48 under 35 U.S.C.§103(a) over Olivier in view of Canale

The Office argues that Olivier in combination with Canale teaches a method and server for processing electronic messages, wherein the message comprises a forwarding restriction indicating (a) whether the message may be forwarded and/or (b) to whom the message may be forwarded, and therefore, Claims 12, 28, and 48 of the instant application are obvious over Olivier in view of Canale.

In order for a rejection under 35 U.S.C.§103(a) to be proper, there must be some suggestion or motivation to modify the reference or to combine the reference teachings, there must be a reasonable expectation of success, and the prior art reference or references must teach or suggest all of the claim limitations. In re Vaeck, 947 F.2d 488 (Fed. Cir. 1991).

Appellants respectfully disagree with the Examiner's position that Olivier and Canale teach all of the claim limitations of Claims 12, 28, and 48.

The Office concedes that Olivier does not teach a forwarding restriction indicating (a) whether the message may be forwarded and/or (b) to whom the message may be forwarded. Instead, the Office asserts that Col. 3, line 54 through Col. 4, line 8 of Canale teach a forwarding restriction indicating to whom the message may be forwarded.

The relied upon portion of Canale recites:

> If user model 113 does not specify a recipient which is of the same kind specified by recipient description 125, mail filter 109 looks to correspondent models 111 to determine where to send mail item 119. There is a correspondent model 111(m) for each of user 105(n)'s frequent correspondents, and like user model 113, each correspondent model 111(m) contains data which mail filter 109 can use together with recipient description 125 to determine which of user 105(n)'s correspondents should receive mail item 119. Mail filter 109 then adds

> the names and e-mail addresses of those correspondents to referral list 127 in mail item 119 and forwards mail item 119 to those correspondents. If they in turn have mail filters 109, they will also filter mail item 119 as just described. In a preferred embodiment, user 105(n) may specify how much control he desires over forwarding. Forwarding may be completely automatic, or mail filter 109 may present user 105(n) with the information from recipient description 125 and a list of the correspondents it has found for forwarding and let user 105(n) select which of the correspondents is to receive the forwarded letter. (Canale, Col. 3, line 56 through Col. 4, line 8)

Appellants believe this interpretation of Canale is improper and out of the context of the teachings of Canale. The cited portion of Canale describes the operation of a mail filter 109 that positively identifies users that are to receive a forwarded message based on the receiving user's preference (which is not restricted) and correspondent models 111 maintained by the user. This particular passage of Canale teaches that a user may control the forwarding options of his/her mail filter 109. The user that receives the message is given the freedom to select correspondents that are to receive the message without any sort of restriction. Each recipient of the mail item 119 is allowed to forward the mail item 119 on to other users without restriction.

In Canale, while a recipient specifier is discussed, it does not restrict access to a communication in a manner similar to that claimed, but is rather used by a mail filter at the "recipient" to determine whether the recipient desires to receive the message.

This teaches away from the subject matter claimed in Claims 12, 28, and 48, since those claims require receiving a message that comprises a forwarding restriction that impacts negatively what users can access or receive a forwarded message. A message with such a restriction identifier allows a sender to control the distribution of his/her message even after the message has been sent as disclosed in an exemplary embodiment discussed at page 5, line 18 through page 6, line 13 of the application as

filed. The mail filter 109 of Canale only teaches positively identifying users that should receive a message. There is no teaching, suggestion, or motivation to have a message that comprises a forwarding restriction indicating (a) whether the message may be forwarded and/or (b) to whom the message may be forwarded, and therefore, Claims 12, 28, and 48 of the instant application are not obvious over Olivier in view of Canale and should therefore be allowed.

2. Rejection of Claims under 35 U.S.C.§102(e) over Olivier

The Office argues that Olivier teaches the method and server for processing electronic messages using a restriction identifier and/or access restriction, and therefore, Claims 1, 3, 5-8, 10-11, 13-17, 19, 21-24, 26-27, 29-31, 36, 37, 39, 41-44, 46-47, and 49 of the instant application are anticipated by Olivier.

Appellants disagree with the Office's interpretation of Olivier and submit that Olivier teach, suggest, or describe all of the claim elements and therefore does not anticipate the pending claims.

2A. Legal Standard of Review

An invention may receive a patent only if it is novel in relation to prior art described in an application for patent filed or patent granted by another. 35 U.S.C. § 102(e).

A prior art reference renders an invention anticipated if it "discloses every feature of the claimed invention, either explicitly or inherently." Hazani v. United States ITC, 126 F.3d 1473, 1477 (Fed. Cir. 1997); see also Schering Corp. v. Geneva Pharms., Inc., 339 F.3d 1373, 1379 (Fed. Cir. 2003).

2B. What the Prior Art Teaches – the Plain Language of Olivier

Olivier is directed to a method for enabling users to exchange group electronic mail by establishing individual profiles and criteria, for determining personalized subsets within a group. *Users establish subscriptions to an electronic mailing list by specifying user profile data and acceptance criteria data to screen other users.* When a user subscribes, a web server establishes and stores an individualized recipient list including each matching subscriber and their degree of one-way or mutual match with the user. When the user then sends a message to the mailing list, an email server retrieves 100% her matches and then optionally filters her recipient list down to a message distribution list *using each recipient's message criteria.* The message is then distributed to matching users. The user may specify acceptance criteria in the matching algorithm. The matching algorithm may be facilitated by including, in the email body or subject line, a keyword in brackets such as "[for sale]". (emphasis added)

Additionally, email archives and information contributions from users are stored in a database. A web server creates an individualized set of web pages for a user from the database, containing contributions only from users in his recipient list. In other embodiments, users apply one-way or mutual criteria matching and message profile criteria to other group forums, such as web-based discussion boards, chat, online clubs, USENET newsgroups, voicemail, instant messaging, web browsing side channel communities, and online gaming rendezvous.

The user can exclude particular subscribers and subjects from his interactions.

The user can override subscription settings when sending a message. The subscription settings are treated as "default settings", and the user can override any of the settings when sending a message. The user could specify this through additional codes in his email message body, or by using a web form when sending the message.

The web form would include access to override those settings. The subscription matching process described in FIG. 5B and its related text are used to determine the distribution list for the present message being sent. The settings are not stored as the user's permanent settings. An example use is in a neighborhood mailing list for a user to send out a "for sale" message to neighbors within 10 miles of him, overriding his usual acceptance criteria data of neighbors within 3 miles of him. This feature would have to exist in conjunction with the previous feature, controlling delivery of reply email messages, so that recipients can answer to the same group.

The system of Olivier is applicable to voice mail.

2C. The Rejection of Claims 1, 3, 5-7, 14, and 15 is improper as Olivier does not teach, suggest, or describe every claim element of Claim 1

It is the Office's position that Olivier teaches the use of a restriction identifier and/or an access restriction. More specifically, with respect to the restriction identifier, the Office asserts that Olivier teaches a message that (I) identifies a recipient and (a) includes a restricting identifier identifying a subset of recipients from among a set of possible recipients, and then (i) when the identified recipient is not within the subset of recipients continues by (A) not providing the identified recipient access to the message and/or (B) notifying the sender that the identified recipient is not within the subset of recipients.

With respect to the access restriction, the Office asserts that Olivier teaches a message that (I) identifies a recipient and includes **(b)** an access restriction indicating a subset of points of access from among a set of points of access to access the message, and then (ii) when the identified at least one recipient attempts to access the message from a point of access not within the subset of points of access, not providing

access to the message to the identified at least one recipient whose point of access is not within the subset of points of access.

In support of this position, the Office asserts that Olivier teaches the above noted features at Col. 3, lines 17-22 and Col. 5, lines 17-65. Appellants respectfully disagree with the Office's assertion that Olivier teaches each and every element of the Independent Claim 1.

The restriction identifier of the present invention can: (i) be a forwarding restriction indicating one or both of whether or not the message may be forwarded and to whom the message may be forwarded; (ii) be an access restriction indicating that the message may be accessed only from predetermined points of access, such as points of access internal to a network; and/or (iii) refer to other conditions besides class of eligible recipients. The restriction identifier impacts ***negatively*** what users can access a particular message or even the way that a user is allowed to access a message. Creating restriction identifiers allows a sender to control the distribution of his/her message even after the message has been sent.

In contrast, it is abundantly clear that in Olivier, it is the end user (i.e. the recipient) that is specifying the acceptance criteria data - ***not*** the sender as set forth in Independent Claims 1. Moreover, Olivier does not teach any situation where an identified recipient is not within the subset of recipients. At most, the acceptance criteria discussed in Olivier creates a subset of recipients from among a set of possible recipients.

Nowhere in Olivier is there a teaching of identifying a recipient that may or may not be a part of a subset of recipients from among a set of possible recipients.

Regarding the access restriction feature and any claim interpretations (e.g., **(I)(b)**(i) and/or **(I)(b)**(ii)) including such a feature, the Office states that the use of

restriction identifiers to prevent access of electronic mail from a set of communication devices otherwise associated with a recipient is disclosed at Fig. 9, col. 3, lines 17-22, col. 5, lines 47-49, and col. 12, lines 59-65 of Olivier. Contrarily, Olivier makes clear that a "recipient" refers to a person or subscriber and not a device. There are no restrictions for a subset of devices, each of which may be associated with the same recipient. Thus, Olivier teaches that a matching subscriber is forwarded the email, even if not addressed specifically to the subscriber. Olivier does not distinguish between which of the matching ***subscriber's devices*** receives the email let alone specify that the matching subscriber cannot access the message at some of that subscriber's message retrieval nodes.

Claims 3, 5-7, 14, and 15 are dependent from Claim 1. Since Olivier does not teach each and every element of Claim 1, dependent Claims 3, 5-7, 14, and 15 are not anticipated by Olivier.

2D. <u>The Rejection of Claims 16, 19, 21- 23, 30, 31, 36, 39, and 41-43 is improper as Olivier does not teach, suggest, or describe every claim element of Claims 16 and 36</u>

In addition to the proffered arguments, and with respect to Independent Claims 16 and 36, Olivier fails to teach, suggest, or describe ***tagging*** a message with a restriction identifier that will ***negatively*** restrict access to that message.

The Office asserts that Col. 12, lines 59-66 of Olivier describe tagging a message with a restriction identifier when a restriction identifier is received from a user. Appellants respectfully disagree with the Office's assertion that Olivier teaches tagging a message with a restriction identifier.

The relied upon portion of Olivier teaches embedding data into a message from an unknown user. Embedded within the message is the user's profile and acceptance criteria data. As discussed above, the acceptance criteria data described in Olivier positively identifies recipients by comparing the acceptance criteria with all other users' profiles. A user's profile that matches the acceptance criteria of the message will be included in the users that receive the message. The recipients of the message are not restricted based on the embedded acceptance criteria but are instead positively identified and provided with the message.

This is an explicit teaching away from a restriction identifier that impacts negatively which users are allowed to receive a message.

Claims 19, 21- 23, 30, and 31 are dependent from Claim 16 and Claims 39 and 41-43 are dependent from Claim 36. Since Olivier does not teach each and every element of Claims 16 and 36, dependent Claims 19, 21-23, 30, 31, 39, and 41-43 are not anticipated by Olivier.

2E. The Rejection of Claims 8, 17, 24, 37, and 44 is Improper as Olivier does not teach, suggest, or describe every claim element of Claims 8, 17, 24, 37, and 44

As noted above, Olivier fails to teach, suggest, or describe a message that comprises a restriction identifier and when an identified recipient (as identified in the message) is not within a subset of recipients (as identified by the restriction identifier), not providing the identified recipient access to the message even though the identified recipient was listed as a recipient in the message as is recited in Claims 8, 17, 24, 37, and 44.

The Office asserts that Col. 3, lines 17-22 and Col. 5, lines 47-49 of Olivier describe not providing the identified recipient access to a message even when the identified recipient was listed as a recipient in the message. Appellants respectfully disagree with the Office's assertion that Olivier teaches such a feature.

The relied upon portion of Olivier teaches the ability of users to exchange high quality messages with other matching users thus resulting in the creation of sub-groups within the mailing list. This is not the same as receiving a message that has an identified recipient and a restriction identifier that ultimately restricts that identified recipient from obtaining access to the message. The restriction identifier of this particular embodiment is provided to ensure that a sending user does not accidentally send a message to an individual that has been identified as restricted from receiving a message, not to help expedite the exchange of messages within particular user sub-groups.

2F. The Rejection of Claims 10, 26, and 46 is Improper as Olivier does not teach, suggest, or describe every claim element of Claims 10, 26, and 46

It is the Office's position that Olivier teaches a message that comprises an age restriction that specifies an age limit of the message. The Office relies upon Col. 14, lines 23-28 of Olivier where a subscription expiration date is discussed. Appellants respectfully disagree with the Office's assertion that a subscription expiration date is a functional equivalent or even inherently similar to an age restriction recited in Claim 10, 26, and 46. While the age restriction of the present invention is associated with the message and may be used to specify an age limit of the message, the subscription expiration date described in Olivier is associated with a user's profile and ***has no connection with a message***.

2G. The Rejection of Claims 11, 27, and 47 is Improper as Olivier does not teach, suggest, or describe every claim element of Claims 11, 27, and 47

It is the Office's position that Olivier teaches a message that comprises a timestamp indicating when a life of a message starts and comparing the expired life of the message with an age restriction to determine whether a message should be deleted and/or delivered. The Office relies upon Col. 14, lines 23-28 and Col. 18, lines 54-64 of Olivier where a subscription expiration is discussed as well as cleanup operations of a database server. Olivier teaches that during database maintenance messages older than n days may be transferred to a secondary database server or secondary computer systems to reclaim disk space. Appellants respectfully submit that this is not disclosure to anticipate the use of a timestamp to determine whether a message should be deleted and/or delivered. As noted above, the subscription expiration date of Olivier is associated with a user profile whereas the age restriction of the present invention is associated with a message.

2H. The Rejection of Claims 13, 29, and 49 is Improper as Olivier does not teach, suggest, or describe every claim element of Claims 13, 29, and 49

As noted above, Olivier fails to teach, suggest, or describe a message that comprises an access restriction. It is clear from the teaching of Olivier that a "recipient" refers to a person or subscriber and not a device. There are no restrictions for a subset of devices, each of which may be associated with the same recipient. The user of an access restriction helps to ensure that certain messages do not leave a particular premises or are not accessed by a restricted device. A particular user may be able to access a certain message from a communication device within an allowable

set of devices but may not be able to access the same message from a device that is restricted by the access restriction.

Nowhere in Olivier is there a discussion of limiting access to a message based on the device that is used to retrieve the message as recited in Claims 13, 29, and 49.

3. Rejection of Claims 9, 25, and 45 under 35 U.S.C.§103(a) over Olivier in view of Tsuei

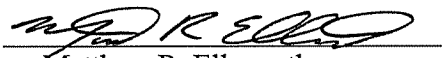
The Office argues that Olivier in combination with Tsuei teaches a method and server for processing electronic messages, wherein the message comprises a restriction identifier and when an identified recipient (as identified in the message) is not within the subset of recipients (as identified by the restriction identifier), the sender is notified that the identified recipient is not within the subset of recipients, and therefore, Claims 9, 25, and 45 of the instant application are obvious over Olivier in view of Tsuei.

As noted above in section 2E the relied upon portion of Olivier teaches the ability of users to exchange high quality messages with other matching users thus resulting in the creation of sub-groups within the mailing list. This is differs from receiving a message that has an identified recipient and a restriction identifier that is designed to restrict that identified recipient from obtaining access to the message. The restriction identifier of this particular embodiment is provided to ensure that a sending user does not accidentally send a message to an individual that has been identified as restricted from receiving a message, not to help expedite the exchange of messages within particular user sub-groups. If such an event occurs, the sending user can be notified that they are attempting or have attempted to send a message to a restricted recipient.

Tsuei does not overcome the shortcomings of Olivier. Rather, Tsuei is directed to a system and methods for managing Internet e-mail address changes, particularly useful for situations where subscribers change Internet service providers. A computer system manages a database of stored records correlating a first e-mail address of an intended recipient, e.g. an old e-mail address, to a second e-mail address, e.g. a new e-mail address of the intended recipient. A program module in the computer system is responsive to an Internet query for accessing the database to determine whether a second e-mail address of the intended recipient is stored in association with a first e-mail address. Another program module is operative for providing the second e-mail address as a response to the query. The query response is communicated to the sender or to the sender's ISP so that an undeliverable message can be resent to the new e-mail address. Also provided in Tsuei are security and authentication measures for ensuring that address change requests are valid and authentic. There is no teaching, suggestion, or description in Tsuei of notifying a sending user that they attempted or are attempting to send a message to a recipient that has been identified as restricted in the restriction identifier. Accordingly, Appellants submit that Claims 9, 25, and 45 are not obvious over Olivier in view of Tsuei.

For at least the reasons elaborated upon in this brief, Appellants submit that the rejection of the pending claims in view of Olivier and combinations of Olivier and other references, should be withdrawn as the Olivier disclosure does not teach all of the elements as claimed and the remaining references cited in combination with Olivier do not overcome the shortcomings of Olivier.

Respectfully submitted,
SHERIDAN ROSS P.C.

By: 

Matthew R. Ellsworth
Registration No. 56,345
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: August 15, 2007

(VIII) CLAIMS APPENDIX

1. A method for processing an electronic message, comprising:

receiving a message from a sender, the message comprising at least one recipient to receive the message and including at least one of a restriction identifier, the restriction identifier identifying a subset of recipients from among a set of possible recipients and an access restriction indicating a subset of points of access from among a set of points of access to access the message;

determining whether each identified at least one recipient is within the subset of recipients corresponding to the restriction identifier; and wherein at least one of the following steps is performed:

(i) when the message comprises the restriction identifier and an identified at least one recipient is not within the subset of recipients, at least one of not providing access to the message to the identified at least one recipient who is not in the subset of recipients and notifying the sender that an identified at least one recipient is not within the subset of recipients; and

(ii) when the message comprises the access restriction and an identified at least one recipient attempts to access the message from a point of access not within the subset of points of access, not providing access to the message to the identified at least one recipient whose point of access is not within the subset of points of access.

2. The method of Claim 1, wherein the message comprises the restriction identifier and the restriction identifier is located in a header of the message.

3. The method of Claim 1, wherein the message comprises the restriction identifier and the restriction identifier is located in a body of the message.

4. The method of Claim 1, wherein the message comprises the restriction identifier and the restriction identifier is located in a trailer of the message.

5. The method of Claim 1, wherein the message comprises the restriction identifier and the restriction identifier is located in an attachment to the message.

6. The method of Claim 1, wherein the message is received by a server associated with at least one recipient from a server associated with the sender.

7. The method of Claim 1, wherein the at least one of the restriction identifier and an access identifier is configured as a flag.

8. The method of Claim 1, wherein the message comprises the restriction identifier and wherein, when an identified at least one recipient is not within the subset of recipients, the step of not providing access to the message to the identified at least one recipient who is not in the subset of recipients is performed.

9. The method of Claim 1, wherein the message comprises the restriction identifier and wherein, when an identified at least one recipient is not within the subset of recipients, the step of notifying the sender that an identified at least one recipient is not within the subset of recipients is performed.

10. The method of Claim 1, wherein the message comprises an age restriction, the age restriction specifying an age limit of the message.

11. The method of Claim 10, wherein the message comprises a timestamp indicating when a life of a message starts and further comprising:

comparing the expired life of the message with the age restriction to determine whether or not to delete and/or deliver the message to the at least one recipient.

12. The method of Claim 1, wherein the message comprises a forwarding restriction indicating at least one of (a) whether the message may be forwarded and (b) to whom the message may be forwarded.

13. The method of Claim 1, wherein the message comprises the access restriction.

14. A computer readable medium operable to perform the steps of Claim 1.

15. A logic circuit operable to perform the steps of Claim 1.

16. A method for processing an electronic message, comprising:

receiving at least part of a message inputted by a user, the at least part of a message comprising at least one recipient to receive the message;

receiving, from the user, a restriction identifier for the at least part of a message, the restriction identifier identifying a subset of recipients from among a set of possible recipients ; and

when a restriction identifier is received, tagging the message with the restriction identifier.

17. The method of Claim 16, wherein, before the message is sent to the at least one recipient, further comprising:

determining whether each identified at least one recipient is within the subset of recipients corresponding to the restriction identifier; and

when an identified at least one recipient is not within the subset of recipients, at least one of not sending the message to the identified at least one recipient who is not in the subset of recipients and notifying the user that an identified at least one recipient is not within the subset of recipients.

18. The method of Claim 16, wherein the restriction identifier is located in a header of the message.

19. The method of Claim 16, wherein the restriction identifier is located in a body of the message.

20. The method of Claim 16, wherein the restriction identifier is located in a trailer of the message.

21. The method of Claim 16, wherein the restriction identifier is located in an attachment to the message.

22. The method of Claim 17, wherein the message is received by a server associated with at least one recipient from a server associated with the sender.

23. The method of Claim 17, wherein the restriction identifier is configured as a flag.

24. The method of Claim 17, wherein, when an identified at least one recipient is not within the subset of recipients, the step of not providing access to the message to the identified at least one recipient who is not in the subset of recipients is performed.

25. The method of Claim 17, wherein, when an identified at least one recipient is not within the subset of recipients, the step of notifying the sender that an identified at least one recipient is not within the subset of recipients is performed.

26. The method of Claim 17, wherein the message comprises an age restriction, the age restriction specifying an age limit of the message.

27. The method of Claim 26, wherein the message comprises a timestamp indicating when a life of a message starts and further comprising:

comparing the expired life of the message with the age restriction to determine whether or not to delete and/or deliver the message to the at least one recipient.

28. The method of Claim 17, wherein the message comprises a forwarding restriction indicating at least one of (a) whether the message may be forwarded and (b) to whom the message may be forwarded.

29. The method of Claim 17, wherein the message comprises an access restriction indicating a subset of points of access from among a set of points of access to access the message, and further comprising:

when an identified at least one recipient attempts to access the message from a point of access not within the subset of points of access, not providing access to the message to the identified at least one recipient whose point of access is not within the subset of points of access.

30. A computer readable medium operable to perform the steps of Claim 16.

31. A logic circuit operable to perform the steps of Claim 16.

36. A server for processing an electronic message, comprising:

an input operable to receive at least part of a message inputted by a user, the at least part of a message comprising at least one recipient to receive the message, and a restriction identifier for the at least part of a message, the restriction identifier identifying a subset of recipients from among a set of possible recipients; and

when a restriction identifier is received, a processor operable to tag the message with the restriction identifier.

37. The system of Claim 36, wherein, before the message is sent to the at least one recipient, the processor is further operable to determine whether each identified at least one recipient is within the subset of recipients corresponding to the restriction identifier and, when an identified at least one recipient is not within the subset of recipients, at least one of not send the message to the identified at least one recipient who is not in the subset of recipients and notify the sender that an identified at least one recipient is not within the subset of recipients.

38. The system of Claim 36, wherein the restriction identifier is located a header of the message.

39. The system of Claim 36, wherein the restriction identifier is located in a body of the message.

40. The system of Claim 36, wherein the restriction identifier is located in a trailer of the message.

41. The system of Claim 36, wherein the restriction identifier is located in an attachment to the message.

42. The system of Claim 36, wherein the message is received by a server associated with at least one recipient from a server associated with the sender.

43. The system of Claim 36, wherein the restriction identifier is configured as a flag.

44. The system of Claim 36, wherein, when an identified at least one recipient is not within the subset of recipients, the function of not providing access to the message to the identified at least one recipient who is not in the subset of recipients is performed.

45. The system of Claim 36, wherein, when an identified at least one recipient is not within the subset of recipients, the function of notifying the sender that an identified at least one recipient is not within the subset of recipients is performed.

46. The system of Claim 36, wherein the message comprises an age restriction, the age restriction specifying an age limit of the message.

47. The system of Claim 46, wherein the message comprises a timestamp indicating when a life of a message starts and the processor is further operable to compare the expired life of the message with the age restriction to determine whether or not to delete and/or deliver the message to the at least one recipient.

48. The system of Claim 36, wherein the message comprises a forwarding restriction indicating at least one of (a) whether the message may be forwarded and (b) to whom the message may be forwarded.

49. The system of Claim 36, wherein the message comprises an access restriction indicating a subset of points of access from among a set of points of access to access the message, and wherein, before allowing access to the message by the at least one recipient, the processor is operable to determine point of access of the at least one recipient and, when the point of access of the at least one recipient is not within the subset of points of access, not allowing access to the message.

(IX) EVIDENCE APPENDIX

Primarily for the convenience of the reader, copies of the documents relied upon by the Examiner as to grounds of rejection to be reviewed on appeal are provided here. These documents include:

Olivier Patent (U.S. Patent No. 6,480,885)

Clarke Patent Application (U.S. Patent App. No. 2003/0065727)

Tsuei Patent (U.S. Patent No. 6,654,779)

Canale Patent (U.S. Patent No. 5,619,648).

(X) RELATED PROCEEDINGS APPENDIX

None.

US006480885B1

(12) **United States Patent**
Olivier

(10) **Patent No.: US 6,480,885 B1**
(45) **Date of Patent: Nov. 12, 2002**

(54) **DYNAMICALLY MATCHING USERS FOR GROUP COMMUNICATIONS BASED ON A THRESHOLD DEGREE OF MATCHING OF SENDER AND RECIPIENT PREDETERMINED ACCEPTANCE CRITERIA**

(76) Inventor: **Michael Olivier**, 2517 Nedson Ct., Suite 200, Mountain View, CA (US) 94043

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/557,681**

(22) Filed: **Apr. 25, 2000**

Related U.S. Application Data

(63) Continuation-in-part of application No. PCT/US99/21589, filed on Sep. 15, 1999.
(60) Provisional application No. 60/100,387, filed on Sep. 15, 1998, provisional application No. 60/115,566, filed on Jan. 12, 1999, and provisional application No. 60/143,947, filed on Jul. 15, 1999.

(51) **Int. Cl.**[7] **G06F 15/16**
(52) **U.S. Cl.** **709/207**; 709/106; 709/202
(58) **Field of Search** 709/106, 202, 709/207

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,513,126	A		4/1996	Harkins et al.
5,555,426	A		9/1996	Johnson et al.
5,694,616	A		12/1997	Johnson et al.
5,796,393	A		8/1998	Macnaughton et al.
5,819,261	A	*	10/1998	Takahashi et al.
5,864,684	A		1/1999	Nielsen
5,909,679	A		6/1999	Hall
5,923,845	A		7/1999	Kamiya et al.
5,959,693	A		9/1999	Geerings
5,999,932	A		12/1999	Paul
6,012,090	A	*	1/2000	Chung et al.
6,047,310	A	*	4/2000	Kamakura et al.

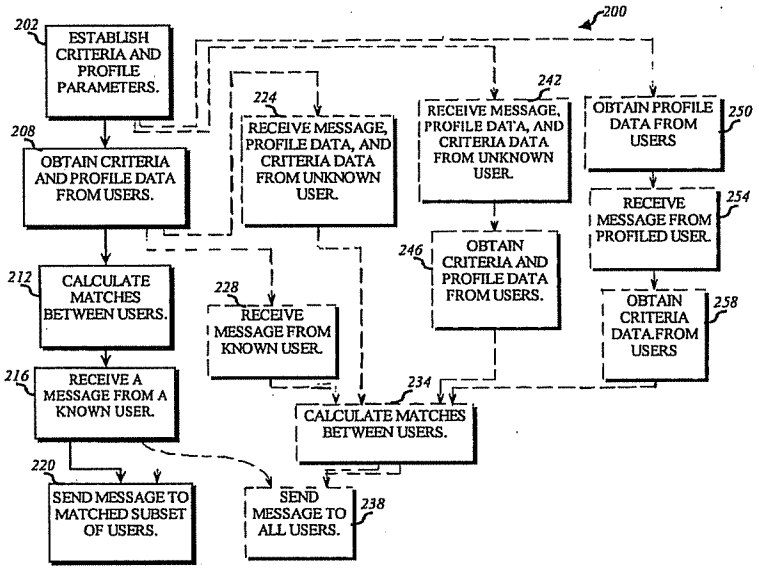
* cited by examiner

Primary Examiner—Le Hien Luu
Assistant Examiner—Stephen Willett
(74) *Attorney, Agent, or Firm*—Oppenheimer, Wolff & Donnelly LLP; Claude A. S. Hamrick

(57) **ABSTRACT**

A method for enabling users to exchange group electronic mail by establishing individual profiles and criteria, for determining personalized subsets within a group. Users establish subscriptions to an electronic mailing list by specifying user profile data and acceptance criteria data to screen other users. When a user subscribes, a web server establishes and stores an individualized recipient list including each matching subscriber and their degree of one-way or mutual match with the user. When the user then sends a message to the mailing list, an email server retrieves 100% her matches and then optionally filters her recipient list down to a message distribution list using each recipient's message criteria. The message is then distributed to matching users. Additionally, email archives and information contributions from users are stored in a database. A web server creates an individualized set of web pages for a user from the database, containing contributions only from users in his recipient list. In other embodiments, users apply one-way or mutual criteria matching and message profile criteria to other group forums, such as web-based discussion boards, chat, online clubs, USENET newsgroups, voicemail, instant messaging, web browsing side channel communities, and online gaming rendezvous.

22 Claims, 15 Drawing Sheets



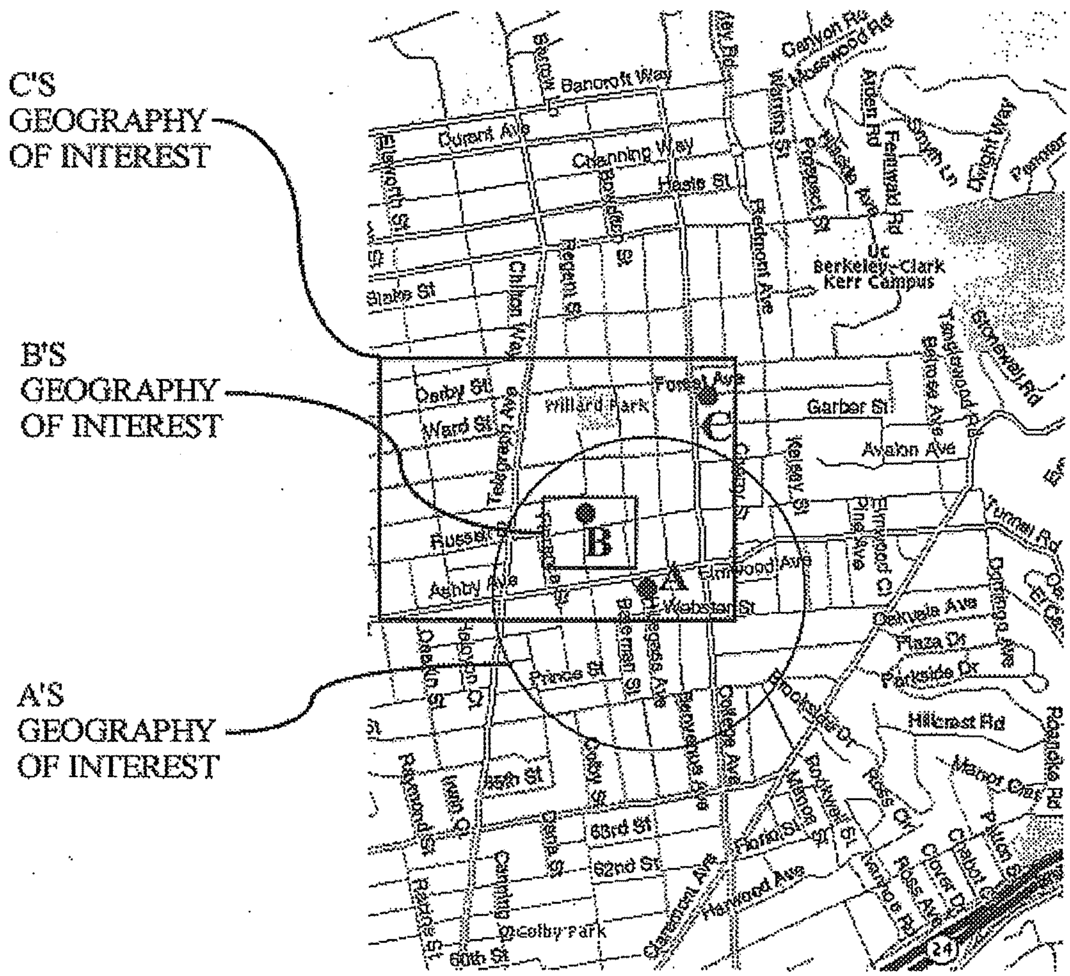

C'S GEOGRAPHY OF INTEREST
B'S GEOGRAPHY OF INTEREST
A'S GEOGRAPHY OF INTEREST
A
B
C

FIG. 1

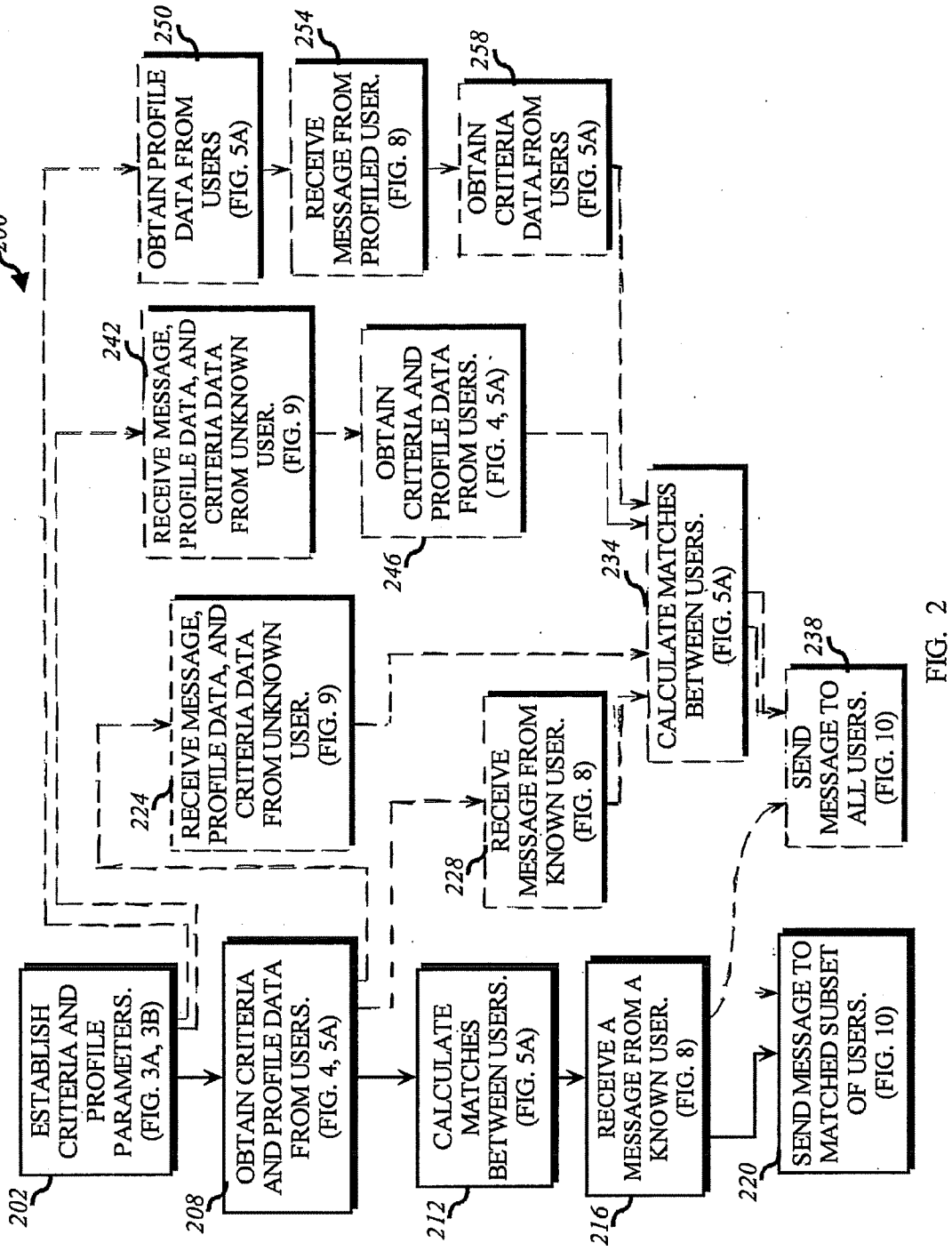

200
ESTABLISH CRITERIA AND PROFILE PARAMETERS. (FIG. 3A, 3B)
202
OBTAIN CRITERIA AND PROFILE DATA FROM USERS. (FIG. 4, 5A)
208
CALCULATE MATCHES BETWEEN USERS. (FIG. 5A)
212
RECEIVE A MESSAGE FROM A KNOWN USER. (FIG. 8)
216
SEND MESSAGE TO MATCHED SUBSET OF USERS. (FIG. 10)
220
224
RECEIVE MESSAGE, PROFILE DATA, AND CRITERIA DATA FROM UNKNOWN USER. (FIG. 9)
228
RECEIVE MESSAGE FROM KNOWN USER. (FIG. 8)
234
CALCULATE MATCHES BETWEEN USERS. (FIG. 5A)
238
SEND MESSAGE TO ALL USERS. (FIG. 10)
242
RECEIVE MESSAGE, PROFILE DATA, AND CRITERIA DATA FROM UNKNOWN USER. (FIG. 9)
246
OBTAIN CRITERIA AND PROFILE DATA FROM USERS. (FIG. 4, 5A)
250
OBTAIN PROFILE DATA FROM USERS (FIG. 5A)
254
RECEIVE MESSAGE FROM PROFILED USER. (FIG. 8)
258
OBTAIN CRITERIA DATA FROM USERS (FIG. 5A)

FIG. 2

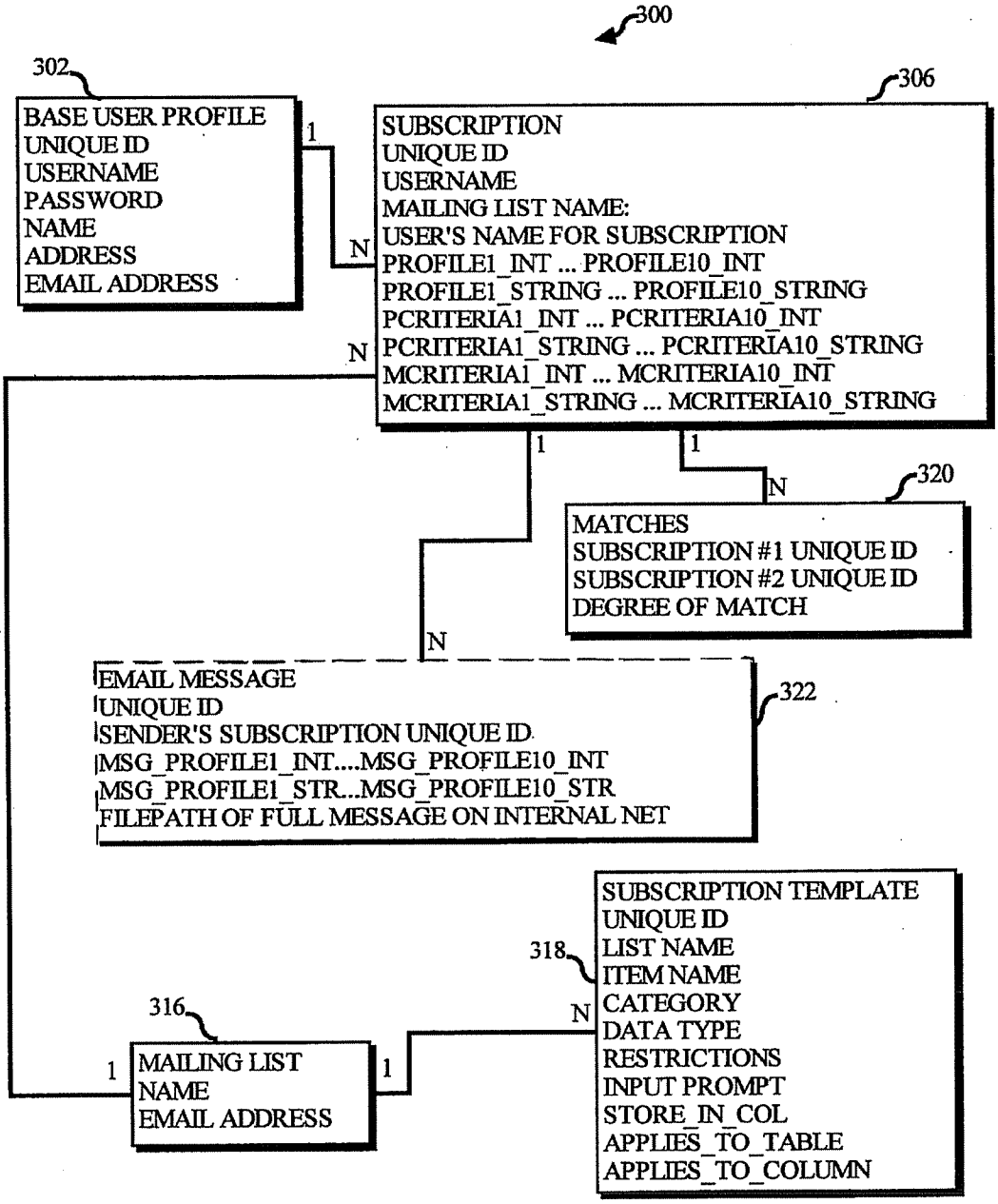

300
302
BASE USER PROFILE
UNIQUE ID
USERNAME
PASSWORD
NAME
ADDRESS
EMAIL ADDRESS
1
N
306
SUBSCRIPTION
UNIQUE ID
USERNAME
MAILING LIST NAME:
USER'S NAME FOR SUBSCRIPTION
PROFILE1_INT ... PROFILE10_INT
PROFILE1_STRING ... PROFILE10_STRING
PCRITERIA1_INT ... PCRITERIA10_INT
PCRITERIA1_STRING ... PCRITERIA10_STRING
MCRITERIA1_INT ... MCRITERIA10_INT
MCRITERIA1_STRING ... MCRITERIA10_STRING
N
1
1
N
320
MATCHES
SUBSCRIPTION #1 UNIQUE ID
SUBSCRIPTION #2 UNIQUE ID
DEGREE OF MATCH
N
EMAIL MESSAGE
UNIQUE ID
SENDER'S SUBSCRIPTION UNIQUE ID
MSG_PROFILE1_INT....MSG_PROFILE10_INT
MSG_PROFILE1_STR...MSG_PROFILE10_STR
FILEPATH OF FULL MESSAGE ON INTERNAL NET
322
SUBSCRIPTION TEMPLATE
UNIQUE ID
318
LIST NAME
ITEM NAME
CATEGORY
DATA TYPE
RESTRICTIONS
INPUT PROMPT
STORE_IN_COL
APPLIES_TO_TABLE
APPLIES_TO_COLUMN
N
316
1
MAILING LIST
NAME
EMAIL ADDRESS
1

FIG. 3A

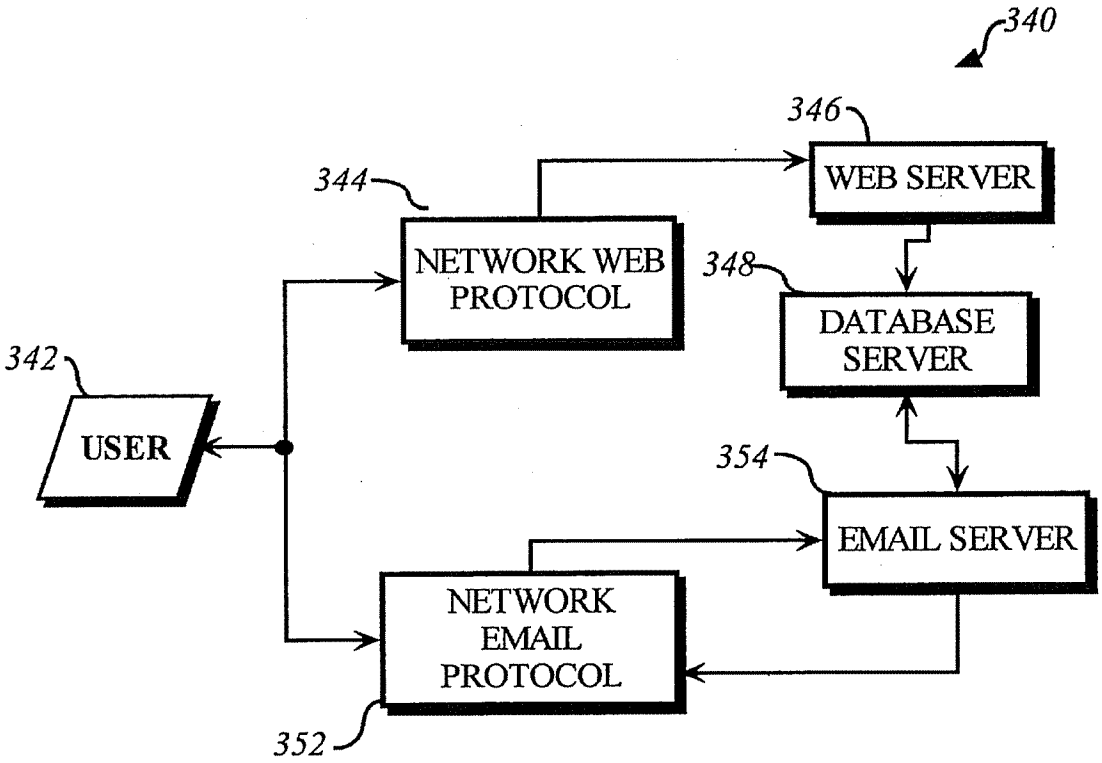

340
346
WEB SERVER
344
NETWORK WEB PROTOCOL
348
DATABASE SERVER
342
USER
354
EMAIL SERVER
NETWORK EMAIL PROTOCOL
352

FIG. 3B

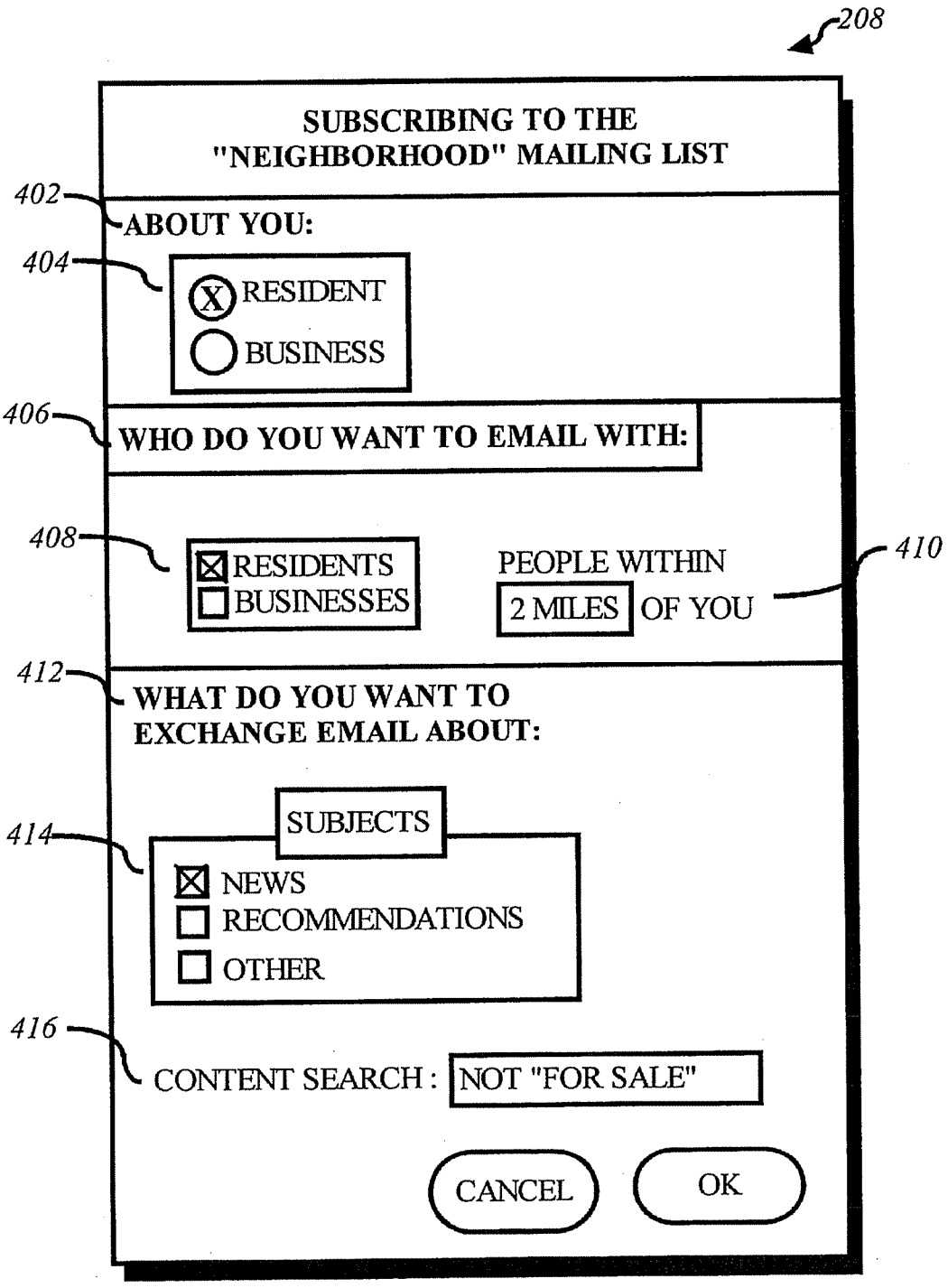

208
SUBSCRIBING TO THE "NEIGHBORHOOD" MAILING LIST
402
ABOUT YOU:
404
RESIDENT
BUSINESS
406
WHO DO YOU WANT TO EMAIL WITH:
408
RESIDENTS
BUSINESSES
PEOPLE WITHIN
2 MILES
OF YOU
410
412
WHAT DO YOU WANT TO EXCHANGE EMAIL ABOUT:
SUBJECTS
414
NEWS
RECOMMENDATIONS
OTHER
416
CONTENT SEARCH :
NOT "FOR SALE"
CANCEL
OK

FIG. 4

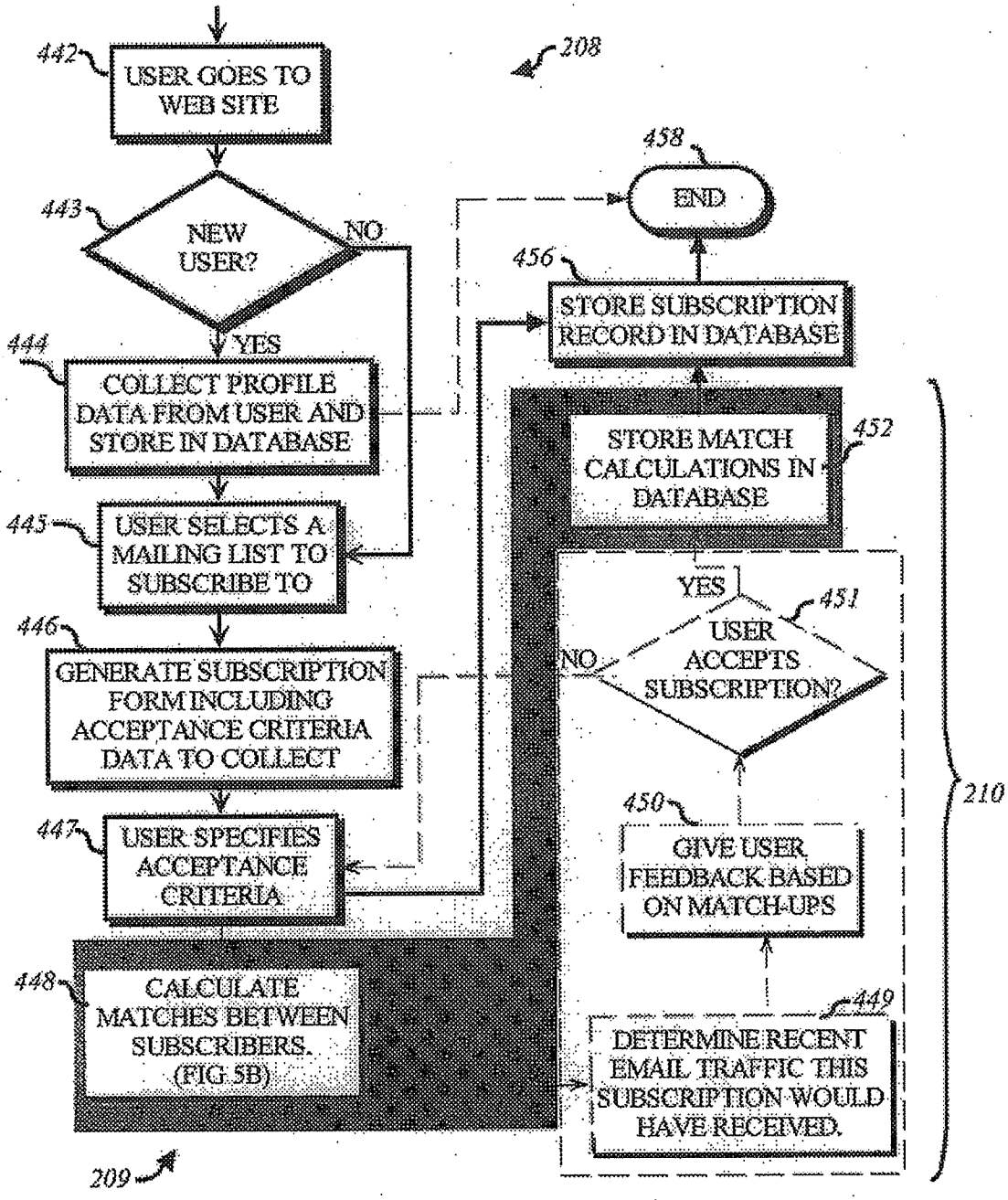

442
USER GOES TO WEB SITE
208
458
END
443
NEW USER?
NO
YES
456
STORE SUBSCRIPTION RECORD IN DATABASE
444
COLLECT PROFILE DATA FROM USER AND STORE IN DATABASE
STORE MATCH CALCULATIONS IN DATABASE
452
445
USER SELECTS A MAILING LIST TO SUBSCRIBE TO
YES
451
USER ACCEPTS SUBSCRIPTION?
NO
446
GENERATE SUBSCRIPTION FORM INCLUDING ACCEPTANCE CRITERIA DATA TO COLLECT
450
GIVE USER FEEDBACK BASED ON MATCH-UPS
210
447
USER SPECIFIES ACCEPTANCE CRITERIA
449
DETERMINE RECENT EMAIL TRAFFIC THIS SUBSCRIPTION WOULD HAVE RECEIVED.
448
CALCULATE MATCHES BETWEEN SUBSCRIBERS. (FIG 5B)
209

FIG. 5A

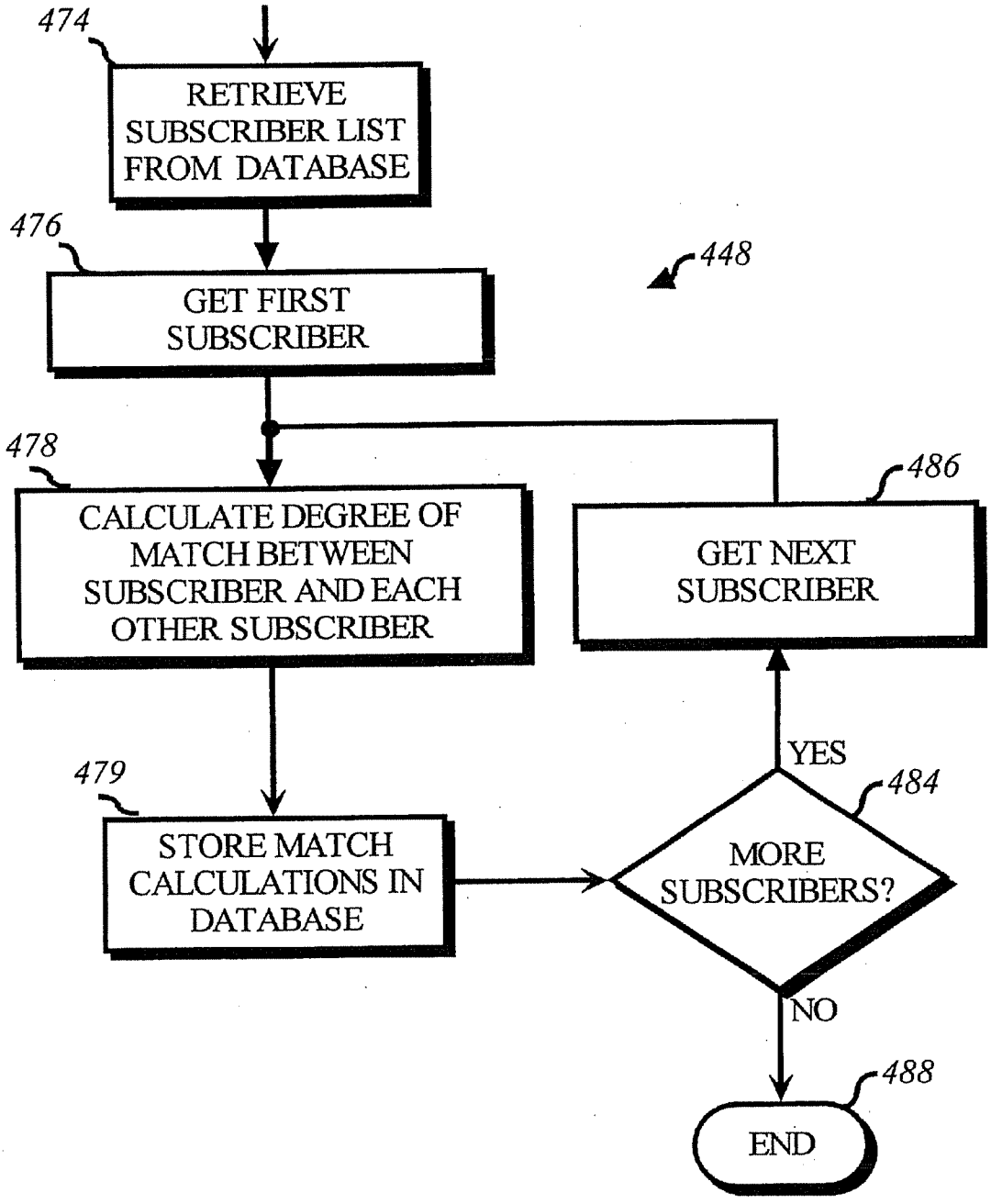

474
RETRIEVE SUBSCRIBER LIST FROM DATABASE
476
GET FIRST SUBSCRIBER
448
478
CALCULATE DEGREE OF MATCH BETWEEN SUBSCRIBER AND EACH OTHER SUBSCRIBER
486
GET NEXT SUBSCRIBER
479
STORE MATCH CALCULATIONS IN DATABASE
YES
484
MORE SUBSCRIBERS?
NO
488
END

FIG. 5B

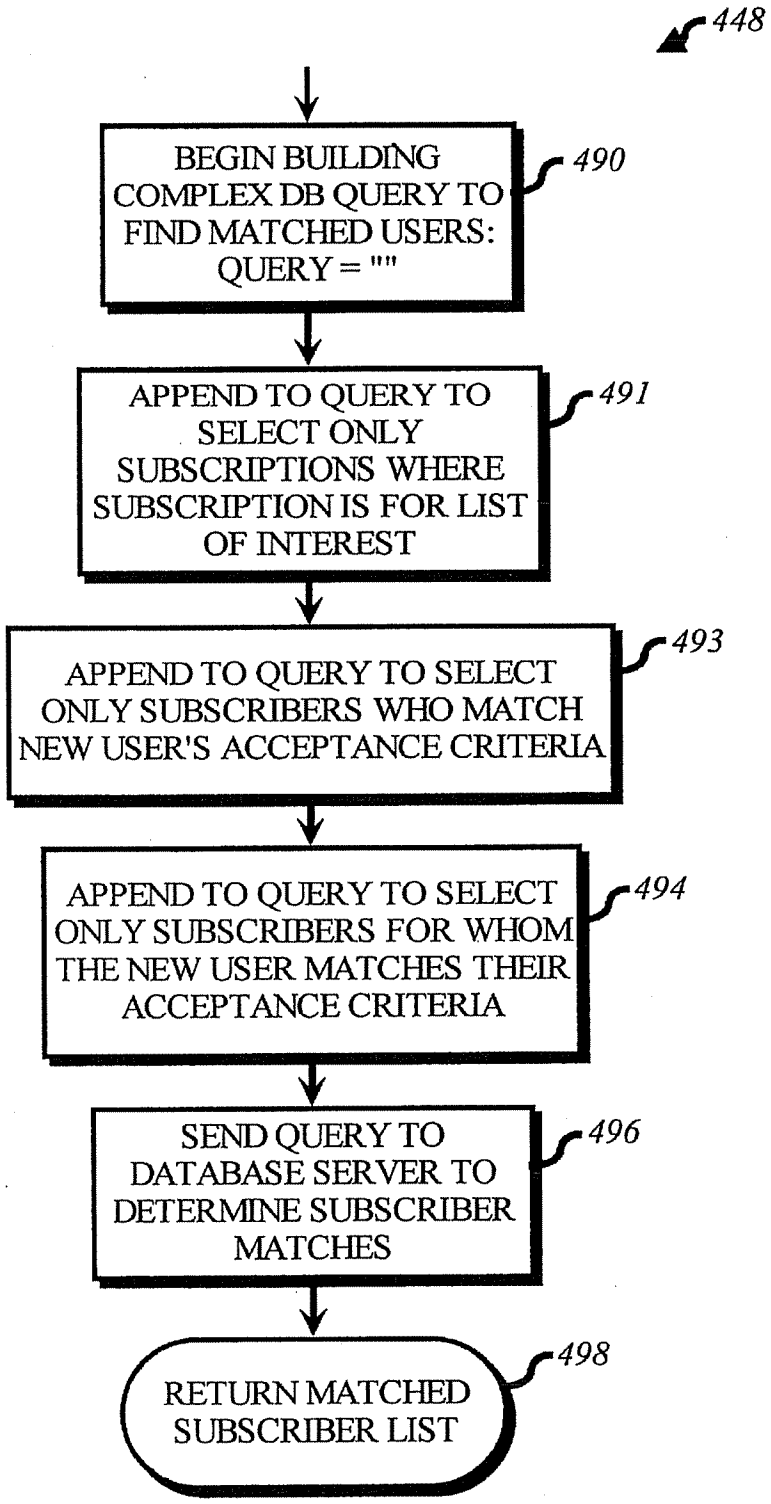

448
BEGIN BUILDING COMPLEX DB QUERY TO FIND MATCHED USERS: QUERY = ""
490
APPEND TO QUERY TO SELECT ONLY SUBSCRIPTIONS WHERE SUBSCRIPTION IS FOR LIST OF INTEREST
491
APPEND TO QUERY TO SELECT ONLY SUBSCRIBERS WHO MATCH NEW USER'S ACCEPTANCE CRITERIA
493
APPEND TO QUERY TO SELECT ONLY SUBSCRIBERS FOR WHOM THE NEW USER MATCHES THEIR ACCEPTANCE CRITERIA
494
SEND QUERY TO DATABASE SERVER TO DETERMINE SUBSCRIBER MATCHES
496
RETURN MATCHED SUBSCRIBER LIST
498

FIG. 6

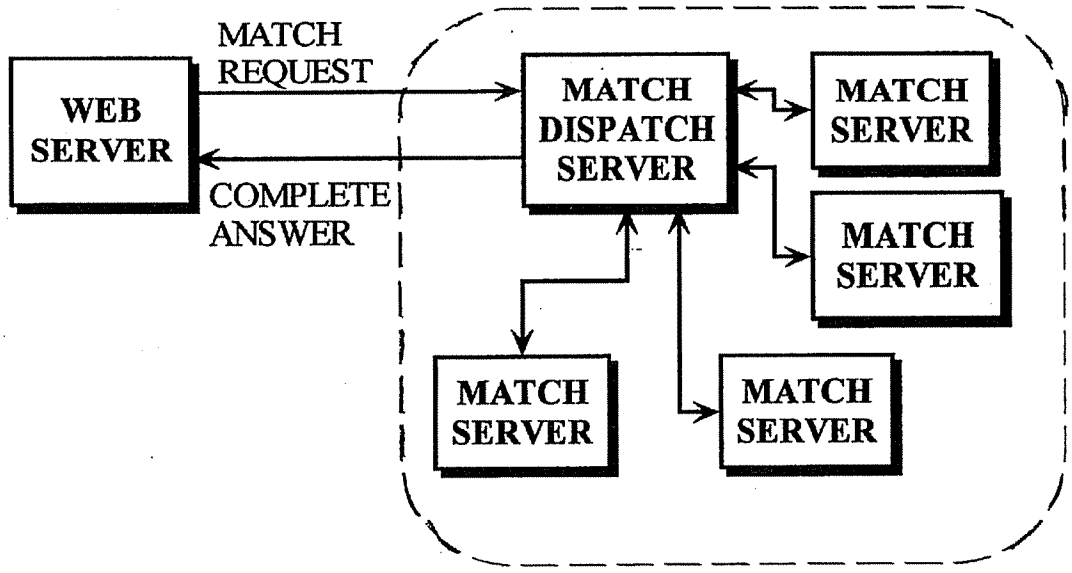
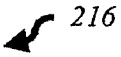

MATCH
REQUEST
WEB
SERVER
COMPLETE
ANSWER
MATCH
DISPATCH
SERVER
MATCH
SERVER
MATCH
SERVER
MATCH
SERVER
MATCH
SERVER

FIG. 7


216

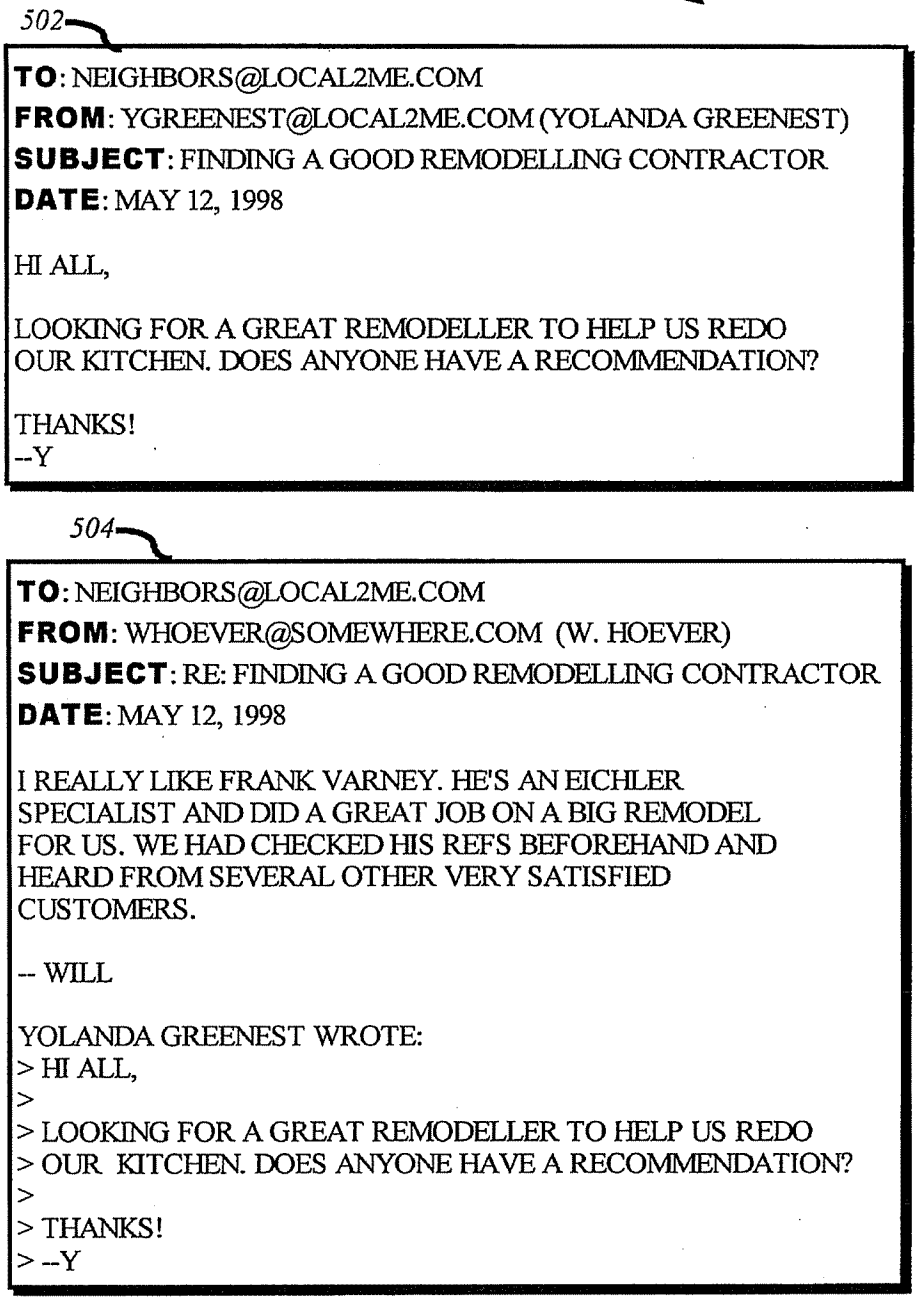

502
TO: NEIGHBORS@LOCAL2ME.COM
FROM: YGREENEST@LOCAL2ME.COM (YOLANDA GREENEST)
SUBJECT: FINDING A GOOD REMODELLING CONTRACTOR
DATE: MAY 12, 1998
HI ALL,
LOOKING FOR A GREAT REMODELLER TO HELP US REDO OUR KITCHEN. DOES ANYONE HAVE A RECOMMENDATION?
THANKS!
--Y
504
TO: NEIGHBORS@LOCAL2ME.COM
FROM: WHOEVER@SOMEWHERE.COM (W. HOEVER)
SUBJECT: RE: FINDING A GOOD REMODELLING CONTRACTOR
DATE: MAY 12, 1998
I REALLY LIKE FRANK VARNEY. HE'S AN EICHLER SPECIALIST AND DID A GREAT JOB ON A BIG REMODEL FOR US. WE HAD CHECKED HIS REFS BEFOREHAND AND HEARD FROM SEVERAL OTHER VERY SATISFIED CUSTOMERS.
-- WILL
YOLANDA GREENEST WROTE:
> HI ALL,
>
> LOOKING FOR A GREAT REMODELLER TO HELP US REDO
> OUR KITCHEN. DOES ANYONE HAVE A RECOMMENDATION?
>
> THANKS!
> --Y

FIG. 8

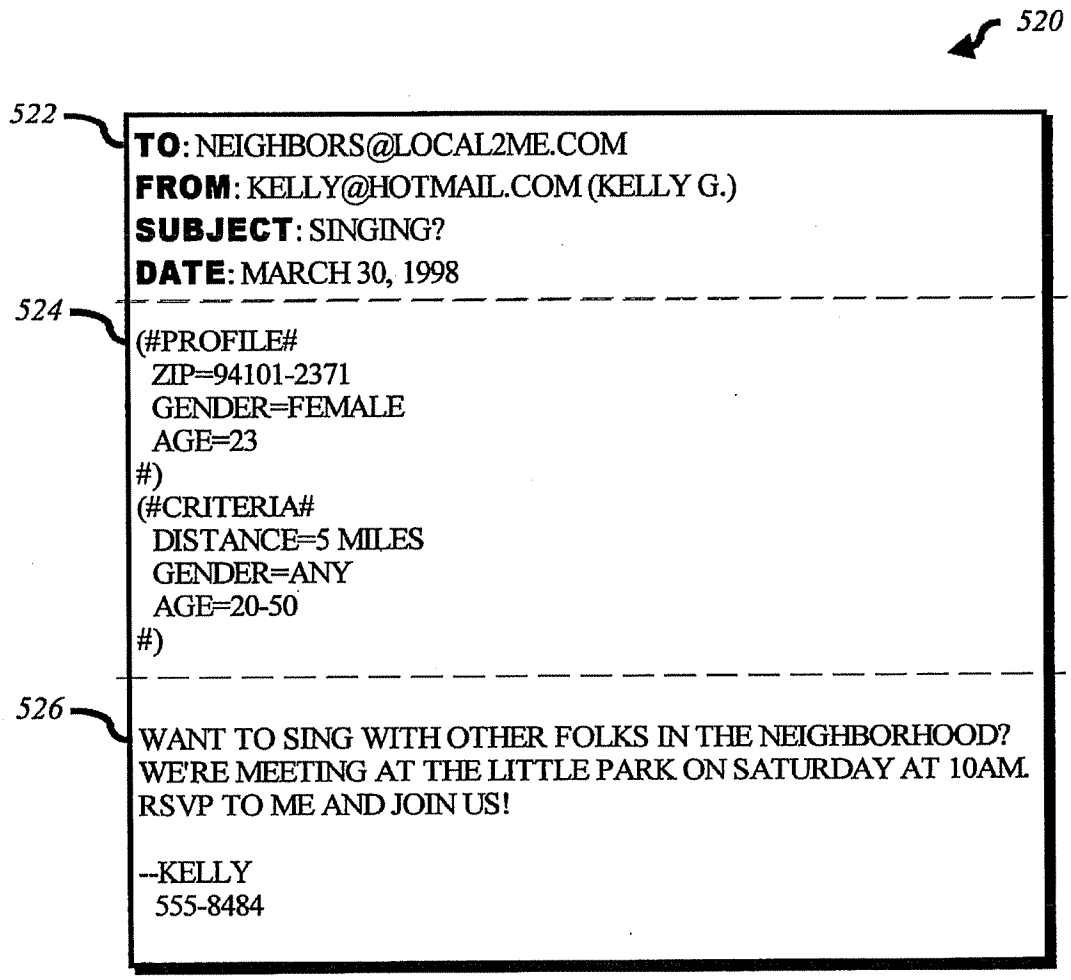

520
522
TO: NEIGHBORS@LOCAL2ME.COM
FROM: KELLY@HOTMAIL.COM (KELLY G.)
SUBJECT: SINGING?
DATE: MARCH 30, 1998
524
(#PROFILE#
ZIP=94101-2371
GENDER=FEMALE
AGE=23
#)
(#CRITERIA#
DISTANCE=5 MILES
GENDER=ANY
AGE=20-50
#)
526
WANT TO SING WITH OTHER FOLKS IN THE NEIGHBORHOOD?
WE'RE MEETING AT THE LITTLE PARK ON SATURDAY AT 10AM.
RSVP TO ME AND JOIN US!
--KELLY
555-8484

FIG. 9

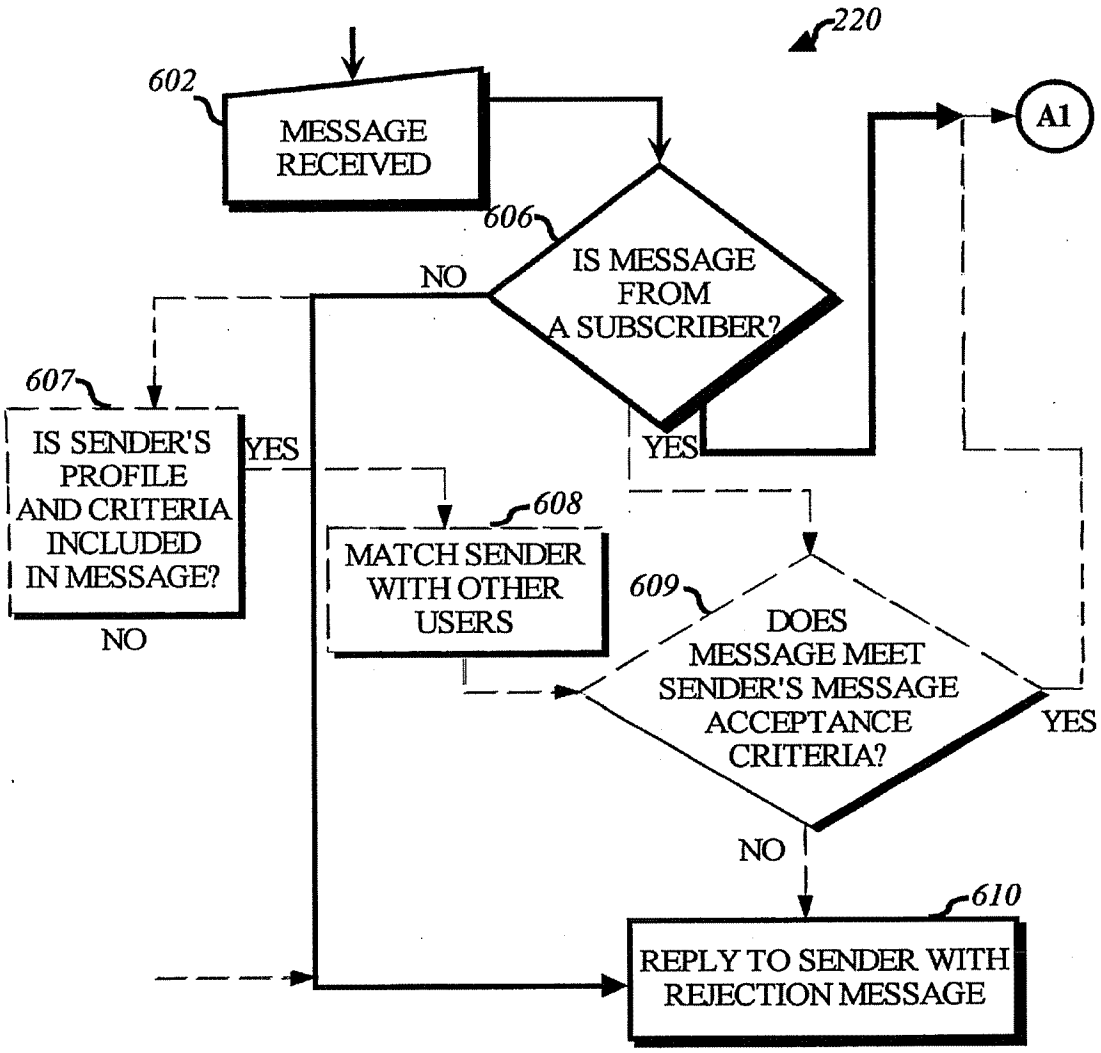

220
602
MESSAGE RECEIVED
606
IS MESSAGE FROM A SUBSCRIBER?
NO
YES
A1
607
IS SENDER'S PROFILE AND CRITERIA INCLUDED IN MESSAGE?
YES
NO
608
MATCH SENDER WITH OTHER USERS
609
DOES MESSAGE MEET SENDER'S MESSAGE ACCEPTANCE CRITERIA?
YES
NO
610
REPLY TO SENDER WITH REJECTION MESSAGE

FIG. 10(1)

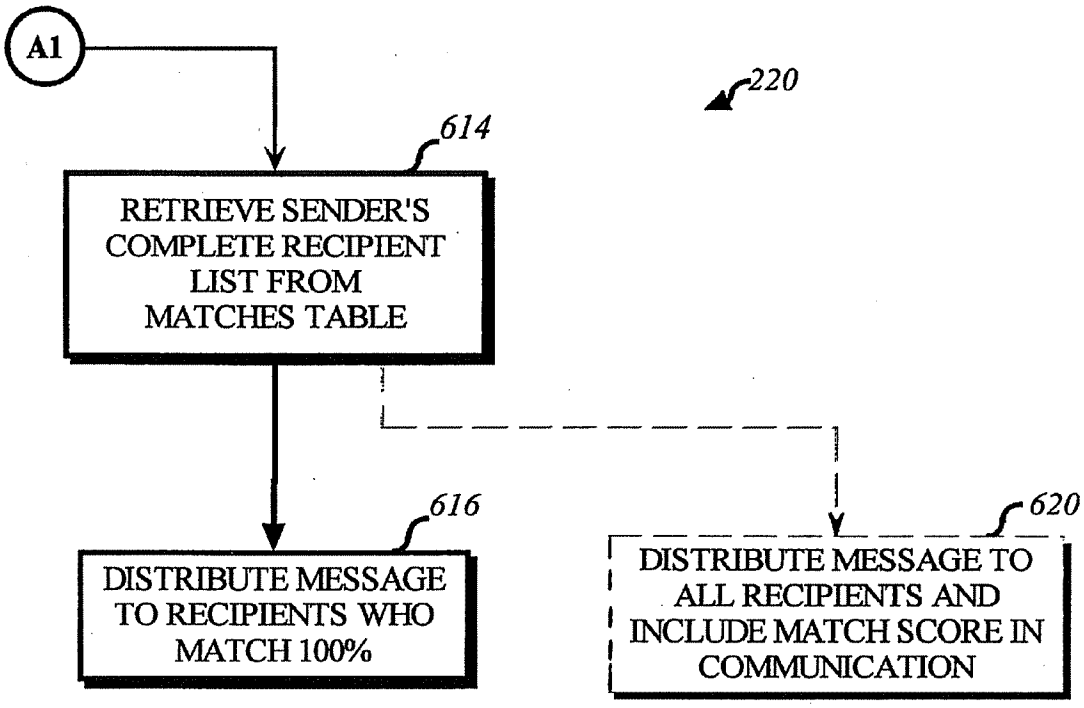

A1
220
614
RETRIEVE SENDER'S COMPLETE RECIPIENT LIST FROM MATCHES TABLE
616
DISTRIBUTE MESSAGE TO RECIPIENTS WHO MATCH 100%
620
DISTRIBUTE MESSAGE TO ALL RECIPIENTS AND INCLUDE MATCH SCORE IN COMMUNICATION

FIG. 10(2)

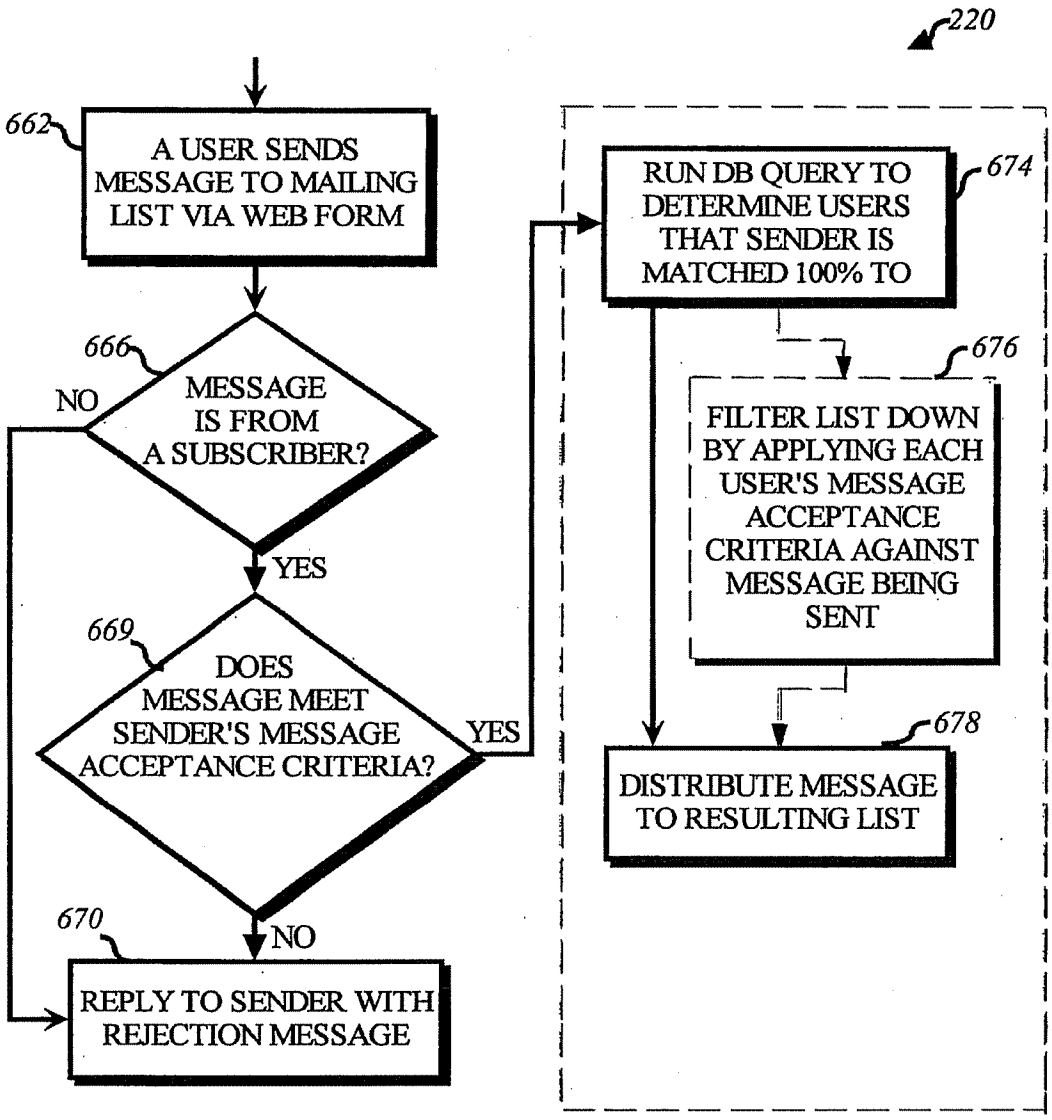

220
662
A USER SENDS MESSAGE TO MAILING LIST VIA WEB FORM
666
MESSAGE IS FROM A SUBSCRIBER?
NO
YES
669
DOES MESSAGE MEET SENDER'S MESSAGE ACCEPTANCE CRITERIA?
YES
NO
670
REPLY TO SENDER WITH REJECTION MESSAGE
674
RUN DB QUERY TO DETERMINE USERS THAT SENDER IS MATCHED 100% TO
676
FILTER LIST DOWN BY APPLYING EACH USER'S MESSAGE ACCEPTANCE CRITERIA AGAINST MESSAGE BEING SENT
678
DISTRIBUTE MESSAGE TO RESULTING LIST

FIG. 11

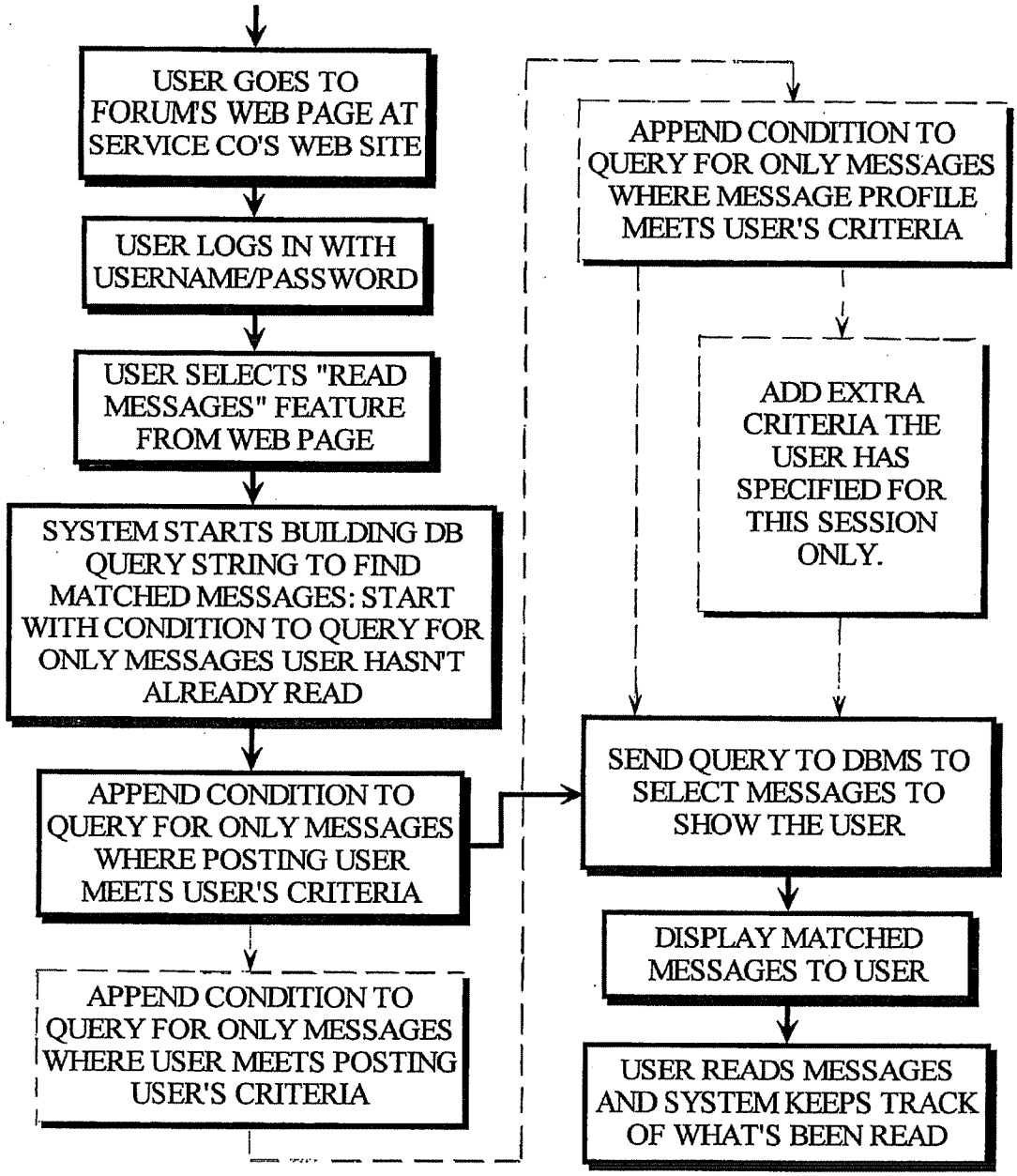

USER GOES TO FORUM'S WEB PAGE AT SERVICE CO'S WEB SITE
USER LOGS IN WITH USERNAME/PASSWORD
USER SELECTS "READ MESSAGES" FEATURE FROM WEB PAGE
SYSTEM STARTS BUILDING DB QUERY STRING TO FIND MATCHED MESSAGES: START WITH CONDITION TO QUERY FOR ONLY MESSAGES USER HASN'T ALREADY READ
APPEND CONDITION TO QUERY FOR ONLY MESSAGES WHERE POSTING USER MEETS USER'S CRITERIA
APPEND CONDITION TO QUERY FOR ONLY MESSAGES WHERE USER MEETS POSTING USER'S CRITERIA
APPEND CONDITION TO QUERY FOR ONLY MESSAGES WHERE MESSAGE PROFILE MEETS USER'S CRITERIA
ADD EXTRA CRITERIA THE USER HAS SPECIFIED FOR THIS SESSION ONLY.
SEND QUERY TO DBMS TO SELECT MESSAGES TO SHOW THE USER
DISPLAY MATCHED MESSAGES TO USER
USER READS MESSAGES AND SYSTEM KEEPS TRACK OF WHAT'S BEEN READ

FIG. 12

DYNAMICALLY MATCHING USERS FOR GROUP COMMUNICATIONS BASED ON A THRESHOLD DEGREE OF MATCHING OF SENDER AND RECIPIENT PREDETERMINED ACCEPTANCE CRITERIA

REFERENCE TO RELATED APPLICATIONS

This application is a Continuation-in Part of PCT/US99/21589 filed Sep. 15, 1999 which claims priority to provisional patent application Ser. No. 60/100,387, filing date Sep. 15, 1998, entitled "Electronic Match-Making Within A Group Using Criteria." This application also claims priority to provisional patent application Ser. No. 60/115,566, filing-date Jan. 12, 1999, entitled "Dynamic Matching™ of Users For Group Communication" and provisional patent application Ser. No. 60/143,947, filing date Jul. 15, 1999, entitled "Dynamic Matching™ of Users For Group Communication."

BACKGROUND OF THE INVENTION

1. Field of Invention

This invention relates to electronic communication within group forums, specifically a process for dynamically matching users for high quality interactions within a group forum by establishing individual user profile data and acceptance criteria data for restricting interaction.

2. Discussion of Prior Art

There are many systems that allow users and groups of users to interact with each other. Electronic forums such as electronic mail, voicemail, USENET newsgroups, web-based discussion boards, and online multi-player gaming services all have such facilities. But none of the systems gives users individualized acceptance criteria parameters for locating high quality matches with other users. Each forum is created with a particular subject or objective in mind, and beyond that all users must follow the boundaries of that forum. It is strictly a "take it or leave it" proposition to the user. There is little opportunity for a user to personalize the forum to meet his own needs.

With electronic mail, users must know the email addresses of those they want to contact. Electronic mailing lists improved on this for group communication by redistributing each message sent to the list's email address out to all subscribers. All users get all messages sent to the list. But there are problems—smaller mailing lists are hard to promote and popularize while larger lists are unwieldy, tending to have many rules of use and/or a high message volume, and a high intimidation factor. In short, users have no control over which users on a list they communicate with. An additional problem is not knowing how much email a subscription will deliver to you. One subscription may bring only a few messages per month while another one fills a user's mailbox with 50 or more messages in a single day.

One common yet inflexible division within a topic is by geographic region. Consider a hypothetical worldwide "jazz" mailing list: If a subscriber wants only to communicate about jazz with people in New York City, he must create a separate mailing list, such as "nyc-jazz". For most users, the work involved in creating and managing a list is prohibitive. Some regional groups may develop their own jazz mailing lists, but such lists are usually tough to advertise and promote. Regional lists are inflexible because they have pre-set borders, e.g., the borders of New York City. That list will not meet the needs of users just outside city limits who

may have a lot in common with those near them just inside city limits, but little in common with those across town. Each user's needs are different and yet the current mailing list systems are inflexible in allowing users to express their needs and wants via customization.

Similarly, there is much work involved in forming a neighborhood mailing list. If someone in a particular neighborhood wants to communicate with neighbors, there are many steps he must take. First he must create a mailing list. Then he may determine the borders of the neighborhood. This is problematic if it is unclear where the borders should be, as is the case with many unnamed neighborhoods. And then he may advertise and evangelize the mailing list to build subscribership. Since most neighborhoods do not have any channel for information distribution (such as a printed newsletter), this is a daunting task.

To extend the example, different people have different wants and needs even within geographically regional communication. In FIG. **1**, one person (A) may want to exchange email with others within a one-mile radius of him. A second person (B) may only want to exchange email with those/on his block. A third person (C) may want only to exchange email with folks in one direction from his house. However, there is currently no way for users to express these desires to control heir participation in a mailing list.

There are countless meaningful acceptance criteria that would benefit users. Consider a parenting mailing list. In general, once a mailing list is formed, it tends to develop its own scope of interest. In this example, the parenting list may develop a very strong trend of discussing infants and toddlers. This can be very limiting for a subscriber who wants to discuss teenagers. That subscriber must delete many unwanted messages and may simply unsubscribe from the list in frustration. She may consider a search for a better list, or she may consider starting a separate mailing list for parents of teenagers, but again the barrier to entry is high. Since the mailing list system cannot leverage information about the ages of children each subscriber is interested in, it cannot deliver to her just those messages about teenagers.

In online gaming, such as "Yahoo! Games", users are able to rendezvous with other users to play multi-player games, such as the card game "hearts". The service provider will often divide the players into several forums based on ability, such as beginner, intermediate, and advanced. But it does, not allow users to specify other acceptance criteria data, such as personality, computer speed, or amount of "chat-style" conversation they want to engage in during a game. Thus users must either live with low quality matches or resort to trial and error, quitting games in the middle, in a search for the characteristics they want in the game. Again the user's only choice is "take it or leave it."

A number of email based news and information services such as InfoBeat provide customized messages to their subscribers, but the messages are only sent by the service itself, not by other users. It is meant for automated information delivery, not interpersonal communication and interaction.

Dating services and employee-employer matching services use criteria and profile information to match people together, but they use those results only for one-on-one communication. hey have not used matching technology for group communication in which each user has their own personalized group.

Although the discussion here has been principally of the interaction provided by electronic mailing lists, other group forums such as USENET newsgroups, web-based discussion

message boards. ah online gaming rendezvous are alternatives that exhibit similar problems.

Thus, a method is needed for creating high quality interactions within electronic forms.

SUMMARY OF THE INVENTION

Briefly, a presently preferred embodiment of the present invention is directed to a method for users to exchange group electronic mail by establishing individual profiles and criteria for determining personalized subsets within a group. Users establish subscriptions to an electronic mailing list by specifying user profile data and acceptance criteria data to screen other users. When a user subscribes, a web server establishes and stores an individualized recipient list including each matching subscriber and their degree of one-way or mutual match with the user.

When the user then 'sends a message to the mailing list, an email server retrieves her 100% matches and then optionally filters her recipient list down to a message distribution list using each recipient's message criteria. The message is then distributed to matching users.

Additionally, email archives and information contributions from users are stored in a database. A web server creates an individualized set of web pages for a user from the database, containing contributions only from users in his recipient list. In other embodiments, users apply one-way or mutual criteria matching and message profile criteria to other group forums, such as web-based discussion boards, chat, online clubs, USENET newsgroups, voicemail, instant messaging, web browsing side channel communities, and online gaming rendezvous.

OBJECTS AND ADVANTAGES

Accordingly, several objects and advantages of the present invention are:

(a) Creates personalized, tunable groups for users, using user profile data and acceptance criteria data they specify. This fundamental novelty greatly empowers and enriches the quality of their communications.

(b) Greatly reduces the quantity of electronic forums such as electronic mailing lists, by making possible a small number very broad forums within which users can create their own niches. For instance, a single jazz mailing list can serve the entire world.

(c) Allows users to very easily create discussion niches of meaning to them. They may want to only email with other senior citizens, or only with those in their city. In the parenting example given earlier, each user could specify the children's age range they would like to discuss. The resulting mailing list is tuned to each user's needs, and gives them a much higher quality of interpersonal contact.

(d) Provides a way for meaningful groups to form automatically, such as neighborhoods.

(e) Provides a way of filtering archived information provided by subscribers into individualized archives. This includes email archives as well as other information such as recommended businesses and web sites.

Additional objects and advantages are to benefit society by creating and uniting a huge number of niche groups, and to meet a compelling and immediate user need to customize email list communications according to individual profiles. By dynamically matching each user's profile data and acceptance criteria data to others, the system creates a customized group for each user, enabling groups to form automatically.

Users need a fluid, flexible, and expressive means of controlling their interactions with others. They need to be able to drastically increase the quality of communication, while controlling the quantity of it. This invention enables these users to customize their communications and interactions.

Further objects and advantages of my invention will become apparent from a consideration of the drawings and ensuing description.

DESCRIPTION OF DRAWINGS

FIG. **1** is an example of neighborhood residents with different geographies of interest.

FIG. **2** is an overview of use of the present invention.

FIG. **3A** is an overview of the invention's system's database.

FIG. **3B** describes the data flow to and from the system servers.

FIG. **4** is an example of a user interface for subscribing to a mailing list.

FIG. **5A** is a flowchart of the user subscription process.

FIG. **5B** is a flowchart depicting the process for determining subscriber matches.

FIG. **6** is an alternative flowchart for determining subscriber matches.

FIG. **7** is another alternative flowchart for determining subscriber matches.

FIG. **8** is an example of users sending email messages to a mailing list.

FIG. **9** is an example of an unknown user sending an email message to a mailing list, including profile and criteria data.

FIG. **10(1)** is a flowchart of the message distribution process to mailing list subscribers.

FIG. **10(2)** is a flowchart of the message distribution process to mailing list subscribers.

FIG. **11** is an alternative flowchart of the message distribution process to mailing list subscribers.

FIG. **12** is a flowchart of an alternative embodiment in which the user reads messages in a web-based discussion forum.

DESCRIPTION OF PREFERRED EMBODIMENTS OF INVENTION

A presently preferred embodiment of the present invention uses exchange of electronic mail as its medium The detailed description to follow will focus on an electronic mailing list system in which subscribers specify acceptance criteria data for engagement and then benefit from the ensuing interaction. It will be clear to those skilled in the art that there are many alternative electronic forums in which the invention could be applied. These include, but are not limited to, voicemail, instant messaging, videoconferencing, online chat, web-based discussion boards, USENET, newsgroups, online gaming, online gaming rendezvous, and unified messaging.

Although the discussion here focuses on the internet network for its preferred embodiment, obviously any automated means for group communication may be used for the present invention.

Overview of Use:

Referring to FIG. **2**, the numeral **200** generally refers to an overview of the use of the present invention. In block **202**, a service provider using the invention initializes the system

for the first time. The service provider initializes a database, or a dedicated part of a database, on a database server available to both an email server and a web server. This is done using a database system, including a schema, data, and a Database Management System (DBMS). The database system is a product such as those from Oracle or Sybase. The service provider sets up the email server to receive and send email on the internet. They also set up the web server to allow subscribers access to the web site via the internet. The database server, email server, and web server each contain a portion of the present invention. In the preferred embodiment the servers are separate, but alternatively their functions could be combined into fewer servers or expanded to more servers.

The service provider then creates one or more electronic mailing lists by adding mailing list records and related records to tables in the database. This is accomplished using a method provided by the database system. The service provider also establishes acceptance criteria data parameters and user profile data parameters for each mailing list which describe what acceptance criteria data and user profile data is to be collected from the users.

At block **208**, a user visits the web site and subscribes to a mailing list, specifying user profile data and acceptance criteria data that control with whom and about what topics they wish to interact. The system stores this and other subscription information in the database. At block **212**, one or more servers calculate the degree of matches between the user and every other user, by doing a one way or two-way match between users, using their user profile data and acceptance criteria data. The results of these match calculations are stored in a database table or other storage.

At block **16** the system receives an email message from a known user addressed to an email address on la server the service provider's server. Note that while in this preferred embodiment we use an email message as the vehicle of a communication, any means of electronic or automated communication may be used in its place. This email address is the address dedicated by the service provider as the email address of the mailing list he subscribed to at block **208**. At block **220** the system determines which mailing list subscribers within the list's subscriber base should receive the email message, by finding in the database the results of the match calculations done in block **212**. It then distributes the email message across the internet to the matching subscribers.

The end result of the process is that users exchange high quality messages with other matching users, and sub-groups form automatically within the mailing list.

To sum up the functionality, consider the following example. Suppose a user Barry wants to send a message about a problem at his child's school. A school mailing list has been established in advance by a service provider hosting the mailing list. Barry first signs up for the school mailing list, specifying his profile and criteria information, including his location and his geography of interest. The system then calculates matches between Barry and other people already on the mailing list based on their profiles and criteria. Barry then writes an email message and addresses it to the email address for his local school mailing list, at the service provider's email server, school@local2me.com. The email server receives the message and retrieves Barry's Match calculations from the database. This describes the other subscribers he is matched with. His message is then sent out to users with whom Barry forms a 100% match, resulting in a satisfying interaction with a subset of users—all the right people.

The remainder of FIG. **2** details several alternative embodiments of the invention that we will now describe.

In an alternative embodiment, block **220** is replaced with block **238**. The message is distributed to all users who are subscribers of the mailing list, and each message indicates the degree of match between the sender and receiver.

In yet another alternative embodiment, the message is received from a known user before the match calculation is done. In this embodiment, blocks **228** and **234** replace blocks **212** and **216**. In step **228** the system receives a message from a known user. Then in block **234** it calculates the matches between users, and uses those results in blocks **220** and **238** in the manner previously discussed.

In still another alternative embodiment, the message received is from an unknown user, and contains user profile data and acceptance criteria data encoded within the message. Blocks **224** and **234** replace blocks **212** and **216**. At block **224**, the system receives a communication from an unknown user, including the message content, user profile data, and acceptance criteria data. Then in block **234** it calculates the matches between users, and uses those results in blocks **220** and **238** in the manner previously discussed.

In another alternative embodiment, the system receives a message from an unknown user before obtaining criteria and profile data from other users. Blocks **242**, **246**, and **234** replace blocks **208**, **212**, and **216**. At block **242**, the system receives a communication from an unknown user, including the message content, user profile data, and acceptance criteria data. In block **246** the system obtains acceptance criteria data and user profile data from a multiplicity of users. Then in block **234** it calculates the matches between users, including the unknown user who sent the message, and uses those results in blocks **220** and **238** in the manner previously discussed.

In another alternative embodiment, the system obtains user profile data first, then receives a message from a profiled user, and then obtains acceptance criteria data before calculating matches and sending the message. Blocks **250**, **254**, **258**, and **234** replace blocks **208**, **212**, and **216**. At block **250**, the system obtains user profile data about users via a web form presented to the users, an email message from the users, an inference engine, a search engine, or another source. The system stores this and other subscription information in the database. At block **254** the system receives a message from a profiled user, i.e., a user who has a known profile. The user sending the message will either transmit his acceptance criteria data with the message or he will specify it with other profiled users at block **258**. At block **258**, the system obtains acceptance criteria data about its profiled users by one or more of the methods described for block **250**. In block **234** the system then calculates the matches between users, including the profiled user who sent the message, and uses those results in blocks **220** and **238** in the manner previously discussed.

Turning to FIG. **3A**, numeral **300** generally refers to a description of the database schema and relationships between entities (Entity/Relationship diagram). The database in this preferred embodiment is a collection of tables of information, as is typically stored in a database product such as Oracle. In the diagram, relationships between tables are shown with '1' or 'n', as will be familiar to those skilled in the art, to indicate the relative number of related records between each pair of tables.

In the description below, we refer to a database record's (or table row's) unique ID. This is also commonly called "Row ID", "Record ID", "Object ID", or "OID" by those skilled in the art, and is simply a unique identifier for each row in a table.

At block **302**, the users table (also referred to as the "base user profile table") contains a collection of base user profile data records. These are records that contain base information about a user, such as name and email address, separate from their subscriptions. Each record also contains a unique ID. In this preferred embodiment, there is only one base user profile data record per user.

At block **306** the subscriptions table contains one record for each subscription entered. Each user can have multiple subscription records, for instance subscribed to a jazz mailing list and a neighborhood mailing list. The subscription table contains the unique ID and unique username of the subscribing user. It also contains the name of the mailing list the subscription is for. Another field allows the user to give the subscription a descriptive name. The table also contains subscription user profile data, which is profile information about the given user specific to this subscription. This information is stored in integers and strings—10 of each type of variable are allocated. Similarly, there are data fields for acceptance criteria data ("pcriteria") describing what this user requires of other users, and message acceptance criteria data ("mcriteria") describing what this user requires of messages he receives. Note that we sometimes refer to message acceptance criteria simply as message criteria. The data in each of these profile and acceptance criteria fields varies between mailing lists. The fields can be interpreted by examining the Subscription Template table, discussed below.

The term "user profile" is used here and below to refer to the combination of both a user's base user profile and the subscription user profile. Base user profile data is collected once when the user first registers at the service provider's web site. But the subscription user profile data is extra profile information needed just for a particular mailing list—it is collected when the user subscribes to a particular list. The term "user profile acceptance criteria" refers to acceptance criteria data related to both the base user profile and the subscription user profile.

At block **316** the mailing lists table contains a record for each mailing list in the system. The service provider, using an access method provided by the database system creates these records. Bach record contains a user-presentable name and an email address for the mailing list.

Block **318** refers to the Subscription Template table. This table defines the user profile data parameters and acceptance criteria data parameters that describe the user profile data and acceptance criteria data needed from each user for each mailing list. These parameters act as templates for data to later be obtained and associated with users. This table also describes where the user profile data and acceptance criteria data are stored in the subscription table, and what user profile data each acceptance criterion refers to. Each row correlates to one piece of user profile data or acceptance criteria data. A unique ID is available for each record. List name is the name of the mailing list. Item name is the name of the item. Category describes the type of template this is: user profile, user profile acceptance criteria, message profile, or message profile acceptance criteria. Data type describes the type of data being collected. The restrictions field describes any restrictions for data entry (e.g., a number between 1 and 10). Prompt is a text string to use when collecting user profile data or acceptance criteria data from the user. $Store_{13}in_{13}col$ describes what column in the subscription table provides storage for this data when collected from the user. $Store_{13}in_{13}col$ also describes what column in the email messages table provides storage for this data when an email message is stored. $Applies_{13}to_{13}table$ and $Applies_{13}to_{13}column$ are only used for acceptance criteria entries in the table. (Not used for user profile entries.) They describe what user profile data the acceptance criteria data applies to. $Applies_{13}to_{13}table$ selects the database table of the profile data that the criteria applies to. This could be either the subscription table, the user table, or the email message table. $Applies_{13}to_{13}column$ identifies the column of interest within that table.

User profile data and acceptance criteria data are closely related. The system compares acceptance criteria data to user profile data to determine subscriber and message matches. A piece of profile data may describe a single data point, such as geographical location, age, or occupation. The corresponding piece of acceptance criteria data may be a range of such data points, such as a geographical area, age range, or set of selected occupations.

At block **320**, the Matches Table keeps track of which subscriptions are matched to each other. The matches table is used so that the time-consuming matching calculation can be done only when needed, with the results stored in this table for quick access. Each row in the table keeps a relation between two matched subscribers. Two subscription unique ID's are stored in each row. A union of searching each of the two subscription unique ID columns for a given subscription's unique ID yields the full set of matching subscriptions for the given subscription. A third column stores the degree of match between the two subscriptions. In the preferred embodiment, this degree of match calculation is a single number representing 0–100%. However, there are many methods of storing such calculations well known to those skilled in the art.

At block **322**, the email archives table is an additional feature to keep an archive of email messages previously processed and distributed by the system. This will be used to give users an estimate of email traffic when they are about to finalize a subscription process, and to allow users to browse the archives via a web interface. A unique ID is available for each record. The sender's subscription unique ID links a message to the sender. $Msg_{13}profile1_{13}int$ to $msg_{13}profile10_{13}int$ and the similar string profile fields store data describing the profile of the message (e.g., topic category is 'recommendations'). These correlate to the message criteria optionally stored in subscription records. The email message content is stored separately in the server's filesystem and its filepath is stored in the DB record.

Turning to FIG. **3B**, the numeral **340** generally refers to the flow of data between users, the email & web servers, and the database server. Block **342** represents a user interacting with the system via email and web protocols via a network. At block **344**, the users interact via a network web protocol **344** with a web server **346**. The web server **346** is software and/or hardware for traditional web serving, plus a portion of the present invention for interacting with users via the web, The web server **346** interacts with a database server **348**. At block **352**, the users **342** use a network email protocol to interact with an email server **354**. Email server **354** is software and hardware for traditional email handling, plus a portion of the present invention for interacting with users via email. The email server **354**, like web server **346**, has access to database server **348**. After processing, email server **354** distributes each message out to via block **352** to multiple users **342**. Note that email server **354**, web server **346**, and database server **348** are three distinct computer systems in this preferred embodiment, but could alternately be combined into fewer computer system or split into more computer systems.

Referring to FIG. **4**, the numeral **208** generally refers to a depiction of an example of a subscription user interface

generated by the system and presented to the user as a web page. Numeral **402** denotes a section collecting subscription user profile data. Numeral **406** denotes a section collecting user profile acceptance criteria data. Numeral **408** refers to some subscription user profile acceptance criteria data, to be compared against subscription user profile data. Numeral **410** refers to some base user profile acceptance criteria data, to be compared against base user profile data. Numeral **412** denotes an optional section allowing the user to specify message acceptance criteria data. Subjects **414** and Content Search **416** are two examples of different kinds of message acceptance criteria data that can be compared against the content and profile of an email message.

Referring to FIG. **5A**, the numeral **208** generally refers to a process of signing a user up for a particular mailing list with the service provider, specifying user profile acceptance criteria data, and storing the subscription.

At block **442**, the user goes to a web site utilizing a portion of this invention. At block **443**, the web server ascertains whether the user is known to the service, or a new user. If he is known, processing, moves to block **445**. If he is not known, the server proceeds to block **444** and presents the user with a new user registration screen. Upon providing profile data such as name, address, email address, age, and occupation, the server stores the base user profile data record in the database. Processing then continues at block **445**. (In an alternative embodiment, instead of continuing to block **445**, processing ends immediately at block **458**, and the user specifies acceptance criteria at a later time.)

At block **445**, the server presents to the user a set of web pages representing a collection of available mailing lists. The user selects a mailing list of interest and indicates via a user interface that he wants to subscribe to it. At block **446**, the server retrieves the mailing list record and related template records from the database. It uses these to build a subscription form, and presents it to the user. The form collects acceptance criteria data from the user. It may also collect additional user profile data specifically needed for the mailing list the user is subscribing to, as specified in the template records in the database. At block **447** the user fills out and submits the subscription form.

At block **456** the server stores the subscription record in the database, including the gathered acceptance criteria. Block **458** ends the process. The next phase of the use of the present invention is when subscribers begin sending email messages out to their mailing lists.

As illustrated by the shaded area designated **209**, block **448** is an optional step that can be done as each subscription is submitted by a user, or at a later time. Thus it is shown as an optional step. At block **448** the server analyzes all subscription records in the subscription table to calculate the degree of matches between the user profile data of the newly subscribing user and the acceptance criteria of each user already subscribed to this particular mailing list. This is depicted in detail in FIG. **5B** and described in detail below.

At block **452** the server stores the subscriber match calculations made in block **448** in the database's matches table. They will be used later to select a subset as the subscriber's personal recipient list for sending out messages, or to indicate to each user with each message the degree of subscriber match between the user and the message sender. Processing then continues at block **456** as described above.

As further illustrated by the bracketed area designated **210**, an alternative embodiment allows user feedback and criteria tuning during the subscription process. This embodiment includes that which is enclosed in the dashed box and also the shaded area designated **209** and described above. In this alternative embodiment, after processing at **208** as described above, the system proceeds to block **449**, where it determines email traffic this subscription would have received in the recent past and the characteristics the user match calculation has produced. It determines the email traffic by matching the new subscriber's message acceptance criteria data to the email archives table in the database for messages sent by matching users as determined in block **448**. The search is further constrained to messages sent to the mailing list of interest. The matching process used is similar to the one that is described in detail below and depicted in FIG. **10**. (In an alternative embodiment (not depicted), in block **449** database sampling or a similar technique known to those skilled in the art is used to provide an estimate as feedback.)

At block **450** the system gives the user a web page or other form of feedback about the subscription the user has specified. That information includes number of users exactly matched to the user and an estimate of the average number of messages per day that the subscription will receive. (In an alternative embodiment not depicted, the system may present more detailed feedback to the user about partial as well as exact matches, rather than just 100% matches.) At block **451** the user chooses whether to accept the subscription as specified or further refine or modify it. If the user accepts the subscription, processing continues at **452** as described above. Otherwise processing returns to block **447**.

In an alternative embodiment (as suggested in FIG. **2**), the user can subscribe to a list dynamically at the time of sending a first message to the list. In that case, the subscription data and possibly the user profile data would be sent via email or other means along with or just ahead of the first message. The subscription feedback steps of the current process (blocks **449–451**) are skipped, and the first message is delivered in accordance with FIG. **10** and the related description below. The subscription may either be stored in the database, or if it is a transient subscription ("one-shot thread" subscription), simply associated with the single email message and not stored in the subscription table. In this latter case, replies to this message back to the mailing list would reach the original sender, but other messages to the mailing list would not.

To summarize by way of example, suppose a user decides to try out a mailing list that uses this invention. He signs up at the service provider's web site, selecting a mailing list about the topic of financial investments. He specifies (user profile acceptance criteria data) he would like to interact with other men of age 40–50 who live within three miles of him and do not have children. Using an optional feature, he selects the subtopics (message criteria) related to internet stocks, junk bonds, and international mutual funds. The system responds with a preview of 38 matching subscribers and five messages per week. He wants more people to interact with, so he increases his age criteria to include men between 35–55. He also increases his distance criteria to five miles. Now the system matches him with 68 people and 12 messages per week, and he accepts the setup. The system stores that subscription; soon he will begin interacting with his matched subscribers.

Using Acceptance Criteria Data to Determine Subscriber Matches:

Turning now to FIG. **5B**, the numeral **448** generally refers to a process of using user-specified acceptance criteria data to calculate subscriber matches. The overall process here is to calculate for each subscriber the degree that his user profile data matches each other subscriber's acceptance criteria data.

At block **474**, the server starts by retrieving a subscriber list for the mailing list from a database query. At bock **476** the server gets the first subscriber on the list. At block **478** the server calculates the degree to which the subscriber's user profile data meets each other subscriber's user profile acceptance criteria data. There are a number of methods well known to those skilled in the, art for making such match calculations.

In the preferred embodiment this is not a two-way match. Even if user X does not want to receive message from user Y, user Y may choose to receive messages from user X if all of Y's acceptance criteria data are met. Acceptance criteria data may include a plethora of different choices, including location, age, sex, hobbies, skills, preferences. While U.S. Pat. No. 5,555,426 by Johnson et al describes a method and apparatus for message dissemination that is based on recipient's acceptance criteria data, its intent and focus are on simple topic keywords and sender identities. It did not comprehend the use described here. The scope of the present invention includes much more comprehensive acceptance criteria data with a significantly different intention, result, and benefit for the users, not suggested by the Johnson patent.

(In an alternative embodiment not depicted, a two-way match process is used in which two match calculations are made. A two-way match, sometimes referred to as a mutual match, is when a user X's acceptance criteria data matches a user Y's user profile data, and user Y's acceptance criteria data matches user X's user profile data. In this alternative embodiment, in addition to the match calculation described above, the system also calculates the degree to which each other subscriber's user profile data meets the subscriber's user profile acceptance criteria data. These calculations are combined into one summary calculation, or are stored separately.)

At block **479** the match calculation data, also sometimes referred to as the match score, is stored in the matches table in the database. At block **484**, the server tests whether there are more subscribers in the list obtained in block **474**. If there are, then at block **486** the server gets the next subscriber and returns to block **478** to continue processing. If there are no more subscribers for whom to do match calculations, processing ends at block **488**.

Next we will focus briefly on some details about the use of acceptance criteria data for selecting subscriber matches for interaction within a group.

Generally, this is the process of determining whether a piece of profile data matches a piece of acceptance criteria data. This process is used either for comparing user profile data to user profile acceptance criteria data, or optionally for comparing message profile data to message profile acceptance criteria data. The system calculates a degree of match between two subscribers, based on one subscriber's user profile data matching to the other acceptance criteria data. Alternatively the matching can be calculated as a two-way match, instead of a one-way match, including both users' acceptance criteria against each other's user profile data.

For each acceptance criterion to test, the server determines the profile data field that matches the current acceptance criterion. The field data may be one of a number of different data types, including text strings, numbers, dates, geographical locations, references to entire other acceptance criteria data records, and lists of any of the aforementioned types. The associated acceptance criteria data are generally ranges of field data, e.g., number range acceptance criterion for number profile data, geographical area of interest acceptance criterion for geographical location profile data, etc. Methods for representing such data types and the type information itself are well known by those skilled in the art.

If an acceptance criterion is a reference to another subscriber's acceptance criteria data, then the entire profile data set becomes the data to be tested against the referenced entire set of acceptance criteria data.

An alternative embodiment to FIG. **5**B is depicted in FIG. **6**. In this embodiment, an SQL database query approach is taken. Block **448** again generally refers to a process of using user-specified acceptance criteria data to determine subscriber matches. At block **490**, the query conditions string is defined to be empty, to begin building a complex query. At block **491**, conditions are appended to the query to select only subscriptions from the subscriptions table that are subscriptions for the target mailing list. Block **493** adds the condition that selects subscribers who match the new subscriber's acceptance criteria data. Block **494** adds the condition that selects subscribers who will accept the new subscriber, per the new subscriber's user profile. At block **496**, the query is sent to the database server. The result back from the database server is a list of subscribers matching all of the conditions. At block **498** the system returns the matched subscribers to the super-process, completing the task of determining matched subscribers.

Another alternative embodiment to FIG. **5**B is depicted in FIG. **7**. In this embodiment, the matching is done through multiple computers operating as a distributed system. All communication between computers is through a standard means such as CORBA. A Match Dispatch Server computer distributes the matching process across a cluster of Match Servers. Each match server handles part of the total number of subscriptions in the system. Each match server keeps its own cached copy of the database data for high-speed access during the matching process. To conduct a match, a client sends a match request to the Match Dispatch Server ("dispatcher"). The dispatcher has a lookup table describing which Match Servers are needed to compute a particular match. The dispatcher returns a list of Match Servers to use in completing a dynamic match. The client then requests those match servers to perform partial matches, and the results are combined for the final answer. The lookup table is centralized on the dispatcher system. Data changes (e.g., from a user tuning his community settings on the web site) will first be stored in an SQL database, and then updates distributed to appropriate server(s). Although FIG. **7** only shows a single dispatcher, multiple redundant dispatchers may be used.

Referring to FIG. **8**, the numeral **216** generally refers to an example of subscribers sending messages to the mailing list email address for distribution to other matching subscribers within the list. The service provider previously designated an email address as the mailing list's address, a practice well known by those skilled in the art. Block **502** is an example of a message sent to "neighbors" mailing list, and block **504** is a response from one of the subscribers who received the original message.

Referring to FIG. **9**, the numeral **520** generally refers to an alternative embodiment to FIG. **8** in which the system receives a message from an unknown user. Embedded within the ordinary email message is the unknown user's profile and criteria data. Block **522** is the header portion of the email message. Block **524** is the profile and criteria data portion of the message, containing all necessary data for cross-matching the unknown user with the known subscribers. The embedded data could alternatively come via an attachment or other means. Or alternatively the entire communication could be transmitted via another means besides

email, such as the HTTP protocol. Block **526** is the body of the message to be distributed.

Process of Distributing Electronic Mail Messages:

Referring to FIG. **10**, the numeral **220** generally refers to a message distribution process, wherein an email message sent by a subscriber is distributed to a subset of subscribers who match the sending user and his message.

At block **602** the system receives an email message from a known user. We'll call this user "sender". (In an alternative embodiment as suggested by FIG. **2**, the message received is from an unknown user.)

In our preferred embodiment, no message profile data is obtained with the message and no matching occurs by message profile and message criteria.

At block **606** the system determines the sender's email address and checks the database or elsewhere to be sure the message is from a subscriber of the specified list. If she is not a subscriber, processing proceeds to block **610** where the message is rejected and a rejection return email is sent to the sender, and processing concludes. If block **606** succeeds, then processing continues at block **614**, where the system retrieves the sender's recipient list from the matches table. In block **616** the system finds the subset of the recipients whose match calculation is a 100% match with the sender. (In an alternative embodiment not depicted, an additional next step at this juncture is to reduce the subset by removing recipients whose message criteria isn't met by the sender's message.)

Finally system distributes the message to the final subset of recipients via the internet or by another method of delivery.

In one alternative embodiment (not depicted), the first line of the body or the subject line of the message received at **602** contains keywords in brackets to specify the message's profile data, e.g., "[for sale]" or "[school]".)

In another alternative embodiment (not depicted), the user fills out a form accessed at the service provider's web site or uses an email-based form. The form includes message body and various form controls such as checkboxes for the user to specify the message's profile data (e.g., this message is about subject "for sale"). The system receives the form data at **602** and processes it in a similar manner.

In yet another alternative embodiment as suggested by FIG. **9**, if in block **606** the sender is not a subscriber, processing proceeds to block **607** where the system checks whether the sender's profile data and criteria data or just the sender's profile data are included in the body of the message. If the data is not included, processing proceeds to block **610** and continues as described above. If the data is included, processing continues at block **608** where the system matches the user against each other user who is a subscriber to the mailing list. This is done using the same process as previously described for calculating matches between users. Processing then continues at block **609**.

In still alternative embodiment, if block **606** succeeds, processing continues at block **609**. At block **609**, the system tests whether the message meets the sender's message profile acceptance criteria data. This is to make sure that the sender is not distributing a message which she herself would block as an incoming message, based on her message profile acceptance criteria data. An example of when this happens is when the user is not accepting "for sale" topics, but sends out a message with a "for sale" message profile. If the message does not meet the sender's message profile acceptance criteria data, then in block **610** the message is rejected and the process ends. If the message meets the acceptance criteria data, then processing continues at block **614**.

In anther alternative embodiment, block **616** is replaced with block **620**. In block **620**, the message is distributed to all recipients in the sender's recipient list, and each sender receives some indication of the match score or generally the degree of match.

FIG. **11** depicts an alternative embodiment to that depicted in FIG. **10**. In this alternative embodiment, the distinction from FIG. **10** is that which is shown in the dashed box. Blocks **614** and **616** of FIG. **10** are replaced by blocks **674–678** of FIG. **11**. Other than that the diagrams and process are identical. In block **674**, a database query is performed to determine matched subscribers, rather than using the pre-calculated matched subscribers stored in the matches table. This would be completed in the same way as previously shown in FIG. **5B** or FIG. **6** and the accompanying description. (In optional block **676**, the resulting list from **674** is pared down by removing subscribers whose message acceptance criteria data indicates they don't want to receive this message.) Finally in block **678** the system distributes the message to the final list of recipients via the internet or by another method of delivery.

Description—Additional Alternative Features

One additional feature would be to allow users the option of specifying a subscription expiration date. The system stores store the expiration date in the subscription field. The system periodically checks the subscriptions table for expired ones. It notifies the user of an expired subscription via email that his subscription has been deleted.

Another feature is to give the subscribing user feedback at subscription time on the identities and/or other info about what subscribers he has been matched up with. This may include email addresses, geographical data such as a graphical map indicating locations of other users.

Another feature is a way for users to be hidden from being revealed to a sender as potential recipients of a message. Some users may desire privacy, and this feature would restrict the processes described herein from revealing that user's identity or other information. The processes are simply, modified to maintain privacy of these users.

Another feature is to allow a user to exclude particular subscribers and subjects from his interactions. Excluding subscribers is similar to chat's "ignore user" feature and is implemented by allowing the user to enter email addresses or user names of users to be ignored. The subscriber matching process described in FIG. **5A**, block **448** and FIG. **5B** are modified to ignore the specified users. The user can also exclude subjects by entering a search string on the subscription tuning web page. The search may be a simple search or complex search predicate. FIG. **10** block **616** is modified to screen out recipients whose search strings match the message content.

Another feature is for the service provider to be able to exclude certain trouble-maker users or groups of users (e.g., hate groups) from the system.

Another feature is a way for users to volunteer to moderate a discussion. A moderator acts as a human filter for inappropriate messages, scanning for "spam" and other messages that shouldn't be sent to the subscribers. A user can only moderate messages she receives through her subscription and she only moderates messages for users that are on her recipient list. A user volunteers on her subscription tuning web page. If in this preferred embodiment there are more than three active moderators, this user is offered only to be put on a moderator wait list. But if there are less than three moderators, this user is considered. There may then be a process of requesting an email vote of approval from the other subscribers this subscriber interacts with. If a vote is

taken, the volunteering is only allowed if that vote comes back substantially positive. Her subscription record is then flagged with a volunteer moderator flag. During message processing, as shown in FIG. **10**, moderators within the recipient distribution list are located and one or more of them is emailed a request to approve the message for distribution. The message is stored in a suspended messages table in the database along with its distribution list until an approval or rejection is returned. If the message isn't approved or rejected after 5 days or another period of time, it is removed from the database and returned to the sender. If a moderator approves the message, it is then sent to the distribution list. If it is rejected, the sender is informed via email. In either case the message is then removed from the suspended messages table.

A variation of the above is a feature to allow the user to specify "ignore moderator." This allows the user, if so desired, to receive all messages regardless of the moderator. Another variation is to allow each user to select from one or more available moderators which moderator he wants, if any.

Another feature is to allow the acceptance criteria data to include a complex search predicate, an example of which is "recommend*OR 'for sale' OR (city and police)". Processes for applying such a search predicate are well know by those skilled in the art. This search could be applied to the message subject and/or content, to the user profile, or to the message profile.

Another feature is to allow more advanced geographical location matching against acceptance criteria data. A mapping product or service is used to recognize street addresses and allow users to specify geographical areas, such as zip code, neighborhood name, city, county, state, region, or an outline drawn on a graphic image of a map. Thus a user can specify the exact geographies of interests and the system can match users based on street addresses and geographies. Alternatives to street address data are the use of street intersection, GPS coordinates, longitude and latitude. If the location is not a specific point, but rather an area, a user would be considered to be generally within that area, and would match another user's geography of interest if the two areas intersected.

Another feature is to allow users to maintain the privacy of their geographical locations by using a small geographical area, such as a ½ mile radius around the user's house, in place of an exact location. This reduces the chance of another user being able to pinpoint someone's exact location. The system would allow the user to specify this as part of their base user profile. It would consider the base user profile data to match another user's location acceptance criteria data if the geographies intersected.

Another feature is allowing two or more subscribers of a particular list to form a group, agreeing to share acceptance criteria data as previously discussed. Each member of the group agrees to apply each other member's acceptance criteria data to everyone except that other member, also previously discussed. Any member can form a group by selecting a user interface element on the webpage for their subscription. The system asks them to name their group, and keeps track of a list of group members within the group's record in a group table in the database. The founding subscriber and anyone else he specifies become the controllers of the group. They must approve all new members via an email or web-based approval mechanism. Then as each member is admitted to the group, each of the group members' subscriptions are recalculated as previously discussed, to update all subscribers' recipient lists based on the change to group acceptance criteria data. Note that recipient lists of subscribers not in the group are also affected. Whenever a group member changes his acceptance criteria data, other group members are notified and the group leader(s) must approve the change or expel the changing member from the group. The group will still interact with users outside the group, but only with users that form a mutual acceptance criteria data match with the compound group acceptance criteria data. Alternatively, the group can simply lock out all non-members from all communication.

Another feature is to allow acceptance criteria data sets outside the scope of a particular subscriber to be used optionally by each subscriber or enforced upon all subscribers. The service provider could set up acceptance criteria data that is associated with an entire mailing list, that specifies that all users must be inside the United States for the list. Or a member or the service provider may specify an acceptance criteria data parameter that when applied rids the system of certain kinds of unwanted commercial email. In either of these cases, or any other similar case, the system allows acceptance criteria data to be named and stored in the database, and for any user to add that acceptance criteria data by reference into their own acceptance criteria data for a subscription.

Another feature is to have the email delivery process control the delivery of reply email messages in a different manner. Replies to an email message go to the distribution list of the original message, rather than the replying subscriber's distribution list. This keeps a discussion with the same group of users, with the potential down-side of some users interacting with each other who don't usually interact. The system stores the email message in the email archive table. It then stores in the database a relationship between the email message sent and the distribution list the message was sent to. The unique ID of the email message's database record is then encoded in the "To" header field of the email message, e.g., "To: neighbors-1354321@local2me.com". When someone responds to the message via their email client's reply all feature, the message is addressed back to that To header field, including the encoded unique ID. When the message arrives at the server, the message is recognized as a reply to an original posting, and the unique ID is extracted from the email address (1354321 in the above example). It then uses the stored distribution list associated with the unique ID, rather than the sender's distribution list, for distribution. The step of checking each recipient's message acceptance criteria data is skipped because the stored distribution list has already done that. The message is then sent to the distribution list. An alternative approach is to have the reply go to the replying subscriber's distribution list, but add some text at the bottom of the message for anyone getting the reply who did not receive the original message it was a reply to. That additional text would be a link to a web page showing the archives of the referenced email message(s).

Another additional feature allows a user to override subscription settings when sending a message. The subscription settings are treated as "default settings", and the user can override any of the settings when sending a message. The user could specify this through additional codes in his email message body, or by using a web form when sending the message. The web form would include access to override those settings. The subscription matching process described in FIG. **5B** and its related text are used to determine the distribution list for the present message being sent. The settings are not stored as the user's permanent settings. An example use is in a neighborhood mailing list for a user to

send out a "for sale" message to neighbors within 10 miles of him, overriding his usual acceptance criteria data of neighbors within 3 miles of him. This feature would have to exist in conjunction with the previous feature, controlling delivery of reply email messages, so that recipients can answer to the same group.

Another additional feature is to allow each list to require approval for subscription. When a user subscribes, another special "approval user" approves or rejects the subscription. This could either be for the whole list, or for a given sub-group within the list as defined by acceptance criteria data. An example is a professional sub-group of a jazz mailing list. Subscribers checking the "Professional" experience checkbox would need to be approved before admittance. In this case, the subscriber is told that his subscription will need to be approved, and his subscription record is stored in a pending subscriptions table. The approval user is emailed with a request for approval. If the approval does not take place within 14 days, the subscriber is automatically rejected by the system.

Another additional feature is to install a process near the beginning of the email distribution process for eliminating unwanted commercial email ("spam"). Such systems are commercially available and are configured independently of this invention. The email server process would allow the service provider to configure it to incorporate a spam elimination process at the appropriate step in the process.

Another additional feature is to offer users a written language preference and translation between languages within a list. A user specifies the language of choice as part of the subscription process. At email distribution time, the email server uses an external language translation process to determine the message's language. For each user whose language preference doesn't match that language, the message is translated before being sent. The translations are grouped so that a translation into a given language happens only once per message. A link to the original message enables review and possible other translations, to account for occasional poor translations.

Another additional feature is for the email server to add an additional text message to each outgoing message. This could be an advertisement or appropriate link to web site content, as determined by the service provider. The system associates header and footer text with the mailing list in the database. The service provider manages that data manually through the database vendor's manual database access interface. The email server grabs that information from the mailing list database entry at the time of message distribution and modifies the message content appropriate Alternatively, the additional text feature may be expanded to allow for distributing different additional text to different sets of users, such as targeted ad insertion. The system associates a number of acceptance criteria data sets described by the service provider with a number of additional text messages. It applies the acceptance criteria data sets one by one to a copy of the distribution list, matching users to the additional text criteria. As each user is matched, the additional text is added to his message and the user is removed from the copy of the distribution list. The last acceptance criteria data set is defined to be a null set, with all remaining users receiving the last additional text message associated with that last null acceptance criteria data set. Thus each user receives only a single additional text message.

Another additional feature allows a user to set up an email alias preference as part of his base user profile. Then each message sent by the user to any mailing list is automatically modified to reflect his email alias rather than the original email address listed in his message. The system also shows this alias instead of his email address at any time his email address would be shown to a user at the web site.

Another additional feature is for the system to determine a user's distribution size threshold based on the user's expertise level. This would warn, for instance, a novice user before sending an email message that would reach more than 200 recipients. The user is asked during registration to rate their computer experience level, and that experience level is matched to thresholds over which the user is warned. During message distribution, the user's threshold is checked for whether there are more recipients on the distribution list than the threshold. If there are, the system informs the user of the size of distribution and asks for confirmation. The system then either distributes, the message or discards it depending on the user's response.

Another additional feature is for the system to verify a user's geographic address when a user subscribes to a mailing list requiring address verification. The mailing list record contains a flag indicating that address verification is required for subscription. When the user subscribes, the system prints a postcard addressed to the user with a special verification code. The system then stores the subscription(s) in a pending subscriptions table in the database. The service provider mails the postcard to the user via the United States Postal Service. Once the user enters the verification code at the web site, the subscription(s) are activated. Alternatively, instead of using a postcard the system allows another subscriber of a given list (e.g., a neighbor) to vouch for the user, for the given list. In that case, the system stores the vouching subscriber's user ID in the subscription record of the new user, and subscribes the new user.

Another additional feature is to show each user individualized web content related to each of his subscription. The web server generates for each user a unique web home page, containing a link for each of his subscriptions. Each of those links leads to a page containing extensive subscriber-created content. The content shown is has been contributed by users matched to the viewing user. In other words, each user only sees subscriber-created content that was created by people he is matched with (and from himself). It displays email archives of messages from the subscribers who match this user's message acceptance criteria data. It also displays other subscriber-created content that matching subscribers have previously contributed to the web site, such as interesting web links, recommendations (such as gardener, electrician, or restaurant), photos, calendar entries, etc. It also displays a way in which this user can add contributions to the site. All content is stored in a user web contribution table in the database. The web site also provides searching of matching subscribers' web sites, from those who have specified a web home page in their base user profile data.

Another additional feature is a periodic process that runs on the database server that performs cleanup operations. It deletes expired subscriptions from subscription table and handles other similar types of cleanup automatically. The system has a parameter that can be set up by the service provider that defines a schedule for performing the database maintenance. It may also transfer messages older than n days to a secondary database server, or move the message bodies to secondary computer systems, to reclaim disk space. In this case, the system must account for this when accessing the email archives.

Another additional feature is to structure the mailing lists into a hierarchy, such that some of the subscription user profile data and acceptance criteria data can be shared

between lists. The system can give the user feedback on the number of users who form partial matches with him based on known acceptance criteria data. For instance, many lists will have a geographic distance component. By extracting that as a common setting for all of those lists, a user can specify early on in the subscription process that he wants to interact with people within two miles of him. He can then browse all of the lists that are in that part of the hierarchy, and see the number of users he is matched to in each of the lists. This gives him very helpful feedback on what lists are active in his immediate area. To accomplish this, the system establishes database relationships to keep track of the hierarchy. It also establishes default values for profile and acceptance criteria data such that partial matches can be determined with partially specified user profile and acceptance criteria data.

Another additional feature is to let a user aggregate several mailing lists together into one "virtual list" for her. She is offered the option of combining two or more subscriptions into one "meta-subscription" that appears as one mailing list in her email box. An example: she wants to combine a "theater" subscription and a "singers" subscription into one meta-subscription she calls "my-arts". Incoming messages to her are then addressed to that list name. When she sends out a message, the underlying mailing lists become message acceptance criteria data which she can check on or off individually to indicate which lists her message should go to. Additionally, for each list she selects, she also needs to specify message acceptance criteria data within that list as per the prior discussion.

Optionally, when a message goes to several lists, recipients belonging to more than one of those lists will orally receive one message (as happens today with newsgroup "cross-postings").

Another additional feature is to allow the user the option of receiving messages for a subscription on the service provider's web site, rather than in her email inbox. In this case the system keeps track of which messages she has and hasn't read, and provides a means of reading and replying to messages.

Another additional feature is to allow users to create ballots to collect votes on any subject from users they are matched to. A user describes the ballot questions via a web site user interface, and the system creates a poll and emails it out to the matched users on the mailing list. The results of the poll are tallied and available for viewing on the service provider's web site. Another additional feature is to provide the user the option of a digest version of messages from a subscription. Rather than each message being delivered separately, a digest message containing multiple messages collected over a short period of time is sent out periodically. Each user specifies when to send out a digest to them, based on time, number of messages waiting, etc. The system collects messages and periodically delivers the digest to the user.

Another additional feature is to provide inexact matching, letting users set thresholds and instructions for different levels of matching. Rather than the previously described 100% match, this allows for partial matching. The user can specify different actions, e.g., they might want scores of 100% delivered via email, those from 70–99% delivered via a daily digest summary email, and those from 60–69% delivered weekly via digest summary email. Scoring the extent of the match also provides the user the ability to literally "turn the volume up or down" on a subscription as a whole. He simply controls a single parameter specifying the threshold for messages to get through.

A related additional feature is to provide the user with a way of expressing the volume of email he desires, and then adjust automatically the score threshold to approximate that volume of traffic. Likewise, the user and/or service provider might want to limit the size of messages (avoiding binaries, pictures, etc.).

Another additional feature is to use more advanced ways of matching acceptance criteria data to user profile data, such as fuzzy logic, artificial intelligence techniques such as discrimination nets, etc. These are techniques well known to those skilled in the art, and can readily be applied within the scope of the present invention.

Another additional feature is a billing mechanism wherein certain "high value" lists are accessible for a fee based on a variety of pricing models, such as monthly charge, volume of messages sent or received, etc. Additional tables would store information to aid in tracking these changes. The billing mechanism would periodically process the information to generate bills for users.

Another additional feature is allowing subscribers to have references within their acceptance criteria data to other subscribers' acceptance criteria data. This is a way for subscribers to use each other's acceptance criteria data. There are many uses for combining acceptance criteria data, with some "real world" parallels. For instance, when musicians form a band, it is often through a process of beginning with each individual's acceptance criteria data, testing whether there is common acceptance criteria data that makes sense, and then finally combining their acceptance criteria data.

In the example below, three subscribers B, C, and D are in different locations and are of different ages. They have met in a "travel" dynamically matched mailing list, and decide to form a discussion niche within the list. The subscribers add references to each other's acceptance criteria data to the records. Their relevant user profile data and acceptance criteria data are:

Subscriber	Location (profile)	Acceptance criteria data for others' locations	Age (profile)	Age Criteria	Other Criteria Records
B	Brazil	California or Denmark or Brazil	20	23–33	C, D
C	California	California or Denmark or Brazil or Germany or New York	26	20–30	B, D
D	Denmark	California or Denmark or Brazil or Venezuela	23	20–27	B, C
Resulting "Outsider" Acceptance criteria data	N/A	California, Brazil, or Denmark	N/A	23–27	N/A

Each subscriber has previously specified location acceptance criteria data and age acceptance criteria data that match the other two subscribers. To form a group, these three subscribers specify to the system to use each other's acceptance criteria data.

Before doing this, the subscribers B, C, and D would each be matched with some other subscribers on the mailing list, which the other members of B–C–D weren't matched with. By incorporating each others' acceptance criteria data they all exclude those other subscribers who do not meet all three sets of acceptance criteria data. A subscriber acceptance criteria data are never used on that subscriber. Since that

subscriber's acceptance criteria data are his acceptance criteria data for others and not for himself, it is not applied to him. Referring to our previous example, subscriber B is 20 years old, but his acceptance criteria data for others is age 23–33, which doesn't include him. Thus when a second subscriber uses a first subscriber's acceptance criteria data, in the preferred embodiment he does not apply that acceptance criteria data to the first subscriber when determining interaction participants. Also in thy preferred embodiment, referenced acceptance criteria data are referring to the combination of a subscriber's user profile acceptance criteria data and message profile acceptance criteria data. Alternatively, the two types of acceptance criteria data could be referenced and used separately between users.

When B combines C's and D's acceptance criteria data with his own, the resulting acceptance criteria data an "outsider" then has to meet is the intersection: California or Denmark or Brazil, and age range 23–30. The combined outsider acceptance criteria data has a modified age range of 23–27. Thus when determining a subscribers' recipient list for a message, outsiders from this group would have to match all of B, C, and D's acceptance criteria data in order to exchange email with any of them. If a fourth "outsider" subscriber "E" from Denmark, age 30, looks for interaction matches in the subscriber list, B, C, and D will not match because of their references to each others' acceptance criteria data. Since D's age acceptance criteria data excludes E, E doesn't match any of them.

An acceptance criterion reference to another users acceptance criteria data can be thought of as a container. Each acceptance criterion inside the referenced user's acceptance criteria data set must be checked. Thus, the system would perform the entire acceptance criteria data process to compare the new set of acceptance criteria data against the given data set. The system must allow for the possibility of circular references to avoid an "endless loop"; techniques for handling this are well known to those skilled in the art.

Since any one user's changes to his criteria impact everyone in the group, the system would include at least two types of groups: "democratic" and "dictatorial". In a democratic group, the system notifies users of any proposed criteria changes, and users have the opportunity to discuss and vote be changes go into effect. In a dictatorial group, one or more of the users are in charge, and approve all criteria changes through a mechanism provided by the system.

There are many other features of electronic mailing list systems such as Majordomo, Listserv, and eGroups.com that are well known to those skilled in the art, that have obvious additional features for the present invention.

Description—Alternative Embodiments for the Present Invention

As discussed earlier, there are many alternative embodiments of the present invention. People need personalized, tunable communities. They need the ability to specify and match up with other people in a variety of electronic forums. This invention is a very powerful way of allowing them to do that—to see only the people they're matched to see. It's like going to a party with all the right people.

One major Difference between different kinds of forums is the latency of the transmissions between parties. Whereas a forum like email has a high latency, a forum such as chat has continuous transmission between the parties, or low latency.

One alternative embodiment is voicemail. Voicemail is very similar to electronic mail in that users typically have a mailbox, and there are group distribution lists, like electronic mailing lists for email. Interaction is non-realtime: each user uses voicemail without any real-time, direct interaction. Thus voicemail, being so similar to email, is a direct application of the present invention to that medium. The user may access the service visually (e.g., web) or orally (e.g., telephone).

Another alternative embodiment for the present invention is unified messaging. Unified messaging is a medium that combines email, voicemail, fax, and potentially other communication services and lets each user select their medium of choice. Sun, Lucent and a number of other companies develop unified messaging solutions. Since unified messaging can always get from other mediums to email, unified messaging is a direct application of the present invention to that medium. These are just different mediums for communication, but they aren't materially different for our purposes. In the preferred embodiment all setup, control, and access to subscriptions, shard data, etc, happens via the web. One modification to that for this alternative is to allow that setup, control, and access to happen via email (or email translated to other unified messaging mediums) instead of the web.

A natural extension to unified messaging is to include telephone, pager, and instant messaging communication, as additional mediums of communication. A user may use different forms of unified messaging for different subscriptions. For instance, a user may want to receive casual neighborhood discussion via email, but receive emergency messages from any neighbor within 5 blocks via text pager, and any communication (e.g., "can I borrow a cup of sugar?") within one block of them, via both instant messaging and fax.

Another alternative embodiment for the present invention is web-based discussion boards. FIG. 12 is la diagram detailing a process for this alternative. Web-based discussion boards are very similar to mailing lists, but users receive and reply to messages (and possibly send messages) through web site rather than an email client application. In other words, rather than messages flowing in and out of the user's email-box, there is instead a bulletin board metaphor with a web interface. The subscription process is substantially the same. The system then keeps track of which messages each user has and hasn't read. The message boards section of the Motley Fool web site (www.fool.com) (Dec. 1998) are an example in the prior art of a web-based discussion board, without benefit of the present invention.

Another alternative embodiment for the present invention is electronic bulletin boards. The most common electronic bulletin boards on the internet are USENET newsgroups (hereafter referred to as newsgroups). The subscription process in this alternative is substantially the same; the main differences come in reading and posting messages. Subscribers post messages through the service provider's server. This could be through a newsgroup server port, or using a web interface, via email to the service provider, etc. Since newsgroup postings are replicated on servers throughout the Internet, there is some efficiency to be gained by encoding some of the database information about the posting user in headers of the posted message. This allows client newsgroup reading programs to do some decoding and matching without having to interact with the service provider's server. Examples of message headers are: "X-Posting-Type: Dynamically Matched Posting", "X-Local2Me-User: joe_{13}hotmail". The system may also encode insensitive profile and acceptance criteria data from the posting user in message headers. Let's call this full set of headers "Dynamic Matching™ Headers." (An example of insensitive user profile data is whether the subscriber considers himself to be

a "professional" or "amateur" in a given field. A home address is an example of sensitive user profile data that, if needed, will have to be evaluated privately at the service provider's server during a user's news reading session.) The client newsgroup reading application may use the Dynamic Matching™ Headers for matching or may require subscribers to read messages through some method provided by a service provider that is utilizing the present invention. In the latter case the client newsgroup reading software knows how to exchange with the server the extra information needed to support the present invention. It informs the server of the identity of the user who is reading messages. The server then only transmits messages whose users form a match and optionally a message acceptance criteria data match with the reading user. Alternatively, the newsgroup reading software may allow the user to see all postings, but highlight matching ones using color, icons, etc. The server in this case transmits additional information to the news reading software about which individual posted messages should have this special highlighting.

If the client newsgroup reading software knows how to interpret Dynamic Matching™ Headers, it may choose to do the matching itself, which may be more efficient than accessing the server for determining match status for each message.

Another alternative embodiment for the present invention is online gaming rendezvous. Services such as "Yahoo! Games" (December 1998) offer forums in which users can meet up for games of cards and other internet-based multiplayer online games. Indeed nearly all commercial computer games to day have some multi-player internet features built in. The typical online gaming forum divides the users into skill levels (their main acceptance criterion) and the users then have to rendezvous via chat to start a game, or jump into an already-formed game. A common experience is to quit part way through a game when you find that your gaming companions are a bad match, in conversation style, speed of play, etc. Applying the present invention, the service provider would offer a host of user profile acceptance criteria data and user profile data to help users rendezvous with the best partners. There is still a registration process for collecting base user profile data. The subscription process is more transient, being more of a "gaming preferences" setup. Following the setup, the user is presented with a set of players who match up with the user based on a mutual acceptance criteria data match. They can then chat, send each other instant messages to invite each other to play, etc. Optionally, when messages are sent they may include, message profile data to allow matched users to apply their message acceptance criteria data. An alternative is to show the user all other users, but denote the matching users through an icon or other graphic highlighting. The system also shows the browsing user games in progress that have open slots, highlighting the users within those games matched to the browsing user. He can then join a game that will have the best chance of being satisfying to him.

Another alternative embodiment for the present invention is online gaming. Many users can play the game simultaneously, but each user only interacts with other users they are mutually matched to. The age software is designed to allow for game play in which each user sees only the other players he is matched to see. This is very similar in implementation to online gaming rendezvous, with additional functionality built into the game play to account for this customized per-player environment.

Another alternative embodiment for the present invention is instant messaging. Instant messaging services such as ICQ, "Yahoo! Pager", AOL Instant Messenger, and Excite PAL allow a user to send another user an immediate text message that pops up on the other user's screen while the user is connected to the messaging system. This is typically when they are connected to the internet and running the messaging client application. Instant messaging applications do not as of yet have the equivalent of electronic mailing lists, i.e., a way to send an instant message to a group of users. Applying the present invention to instant messaging requires no change to the subscription. An additional user interface component in the instant messaging software or on a web page allows the user to see a list of all matching users who are logged on. This happens within the context of a subscription to a particular forum. The user may then choose to send a message to any one user on that list. Sending of messages to an entire matching group is routed through the service provider's instant messaging server, which determines which message recipients will receive the message. It then distributes the message to those recipients. As an example of its use, a user may have two subscriptions set up—she wants to hear from all neighbors within five blocks from her about for sale items, and all neighbors within one block of her about emergencies.

Another alternative embodiment for the present invention is online chat. The subscription process is modified in a way similar to online gaming rendezvous. In today's online chat, users begin by selecting a chat room, and then chatting with everyone in that forum. There is typically a way to ignore specified users. The present invention allows a first user to set up more elaborate acceptance criteria da a only interacting with other users who form a one-way or two-way match with the first user. In the case of a one-way match, the match calculation is between the first user's acceptance criteria data and each other user's user profile data. Alternatively, it allows full chat exchange with all users, but indicates in the user list & message window the degree of match the user has with each other user. For instance, the system could display stronger matches in darker colors and weaker matches in lighter colors. Subscription settings may apply to one or more chat rooms. After setting up a subscription, the user can view a list of chat rooms and see what rooms the people he's matched with are spending their time in. He can then select a room and begin interacting. The message profile and acceptance criteria data are not used. Alternatively, the message profile and acceptance criteria data are used to help users communicate about specific subjects. In that case the system queries the user for message profile data if it cannot be determined automatically.

Another alternative embodiment for the present invention is video conferencing. This is similar to online chat and online gaming rendezvous. The invention is used for finding good videoconferencing partners within a given forum, by either highlighting matching users or only showing matching users. The present invention can be used with either one on one video conferencing, or with group video conferencing. In a group setting, each user conferences with many matching users at once, limited only by the limitations of number of simultaneous user connections in the video conferencing system. Message profiles and message profile acceptance criteria data are not used.

Another alternative embodiment for the present invention is audio conferencing, or "party line." This is an obvious extension of online chat, and similar to video conferencing, wherein multiple users have an audio-only real-time connection to each other in a group setting. This is implemented in substantially the same manner as video conferencing.

Another alterative embodiment for the present invention is online clubs and communities, such as "Yahoo! Clubs"

(Dec. 1998). In these services, a group forms around a theme, and users can chat, post messages to a discussion board, share web links of interest, etc., within that group. By using the present invention, the user can create a personal, tunable niche within the group. The subscription process is the same: after selecting a club, a user can specify his acceptance criteria data within the club. The user then only sees content (chat, message postings, web links, pictures, calendar entries, etc.) of other users who form a match with the user. The chat portion is handled as discussed in the online chat application above. Message postings are handled as described in web-based discussion boards above. Other areas are handled in a similar fashion. Alternatively, the system may allow for one-way acceptance criteria data application: the first user sees content from second users who the first user's acceptance criteria data matches, without regard to the second users' acceptance criteria data. Another alternative process is for to allow moderators, club owners, and other "authorities" to view all messages, even if ere is no mutual acceptance criteria data match.

Another alternative embodiment is web surfing community forums. These forums provide a means for users to exchange messages with each other based on the web sites they are viewing. This service can be provided independently of the web sites that users are posting messages to. This is done through web browser plug-ins and other new technology that allow the exchanged messages to be stored somewhere other than the currently-viewed web site. When users are browsing that site or a particular page at that site, the messages are retrieved from the independent data store and displayed to the user.

In this embodiment, the message exchange may happen in real-time (e.g., chat) or time-shifted (e.g., posting messages). For example, users at a site such as CNN.com could communicate with other users who are on that site at the same time, or who come to the site at other times. The present invention is modified to use the web site address (e.g., www.local2me.com) the user is viewing to match the user with other users. Alternatively it could use the address of a specific page being viewed within the web site (e.g., www.local2me.com/community/internet.html).

For real-time exchange in this embodiment, the web site or page the user is viewing is user profile data. Users can set as part of their user profile acceptance criteria data one or many web pages or web sites. As an example, a user at CNN.com's user profile data would include CNN.com as his currently viewed web site (or alternatively a page within the site). His user profile acceptance criteria data could include all users at CNN.com, ABCsports.com, MSNBC.com, and PBS.org. For time-shifted message exchange, the web site or page the user is vie wing when he posts a message is stored as part of the message profile data (not the user profile data). Other users can set as part of their message profile acceptance criteria data one or many web pages or sites.

An example: a user X goes to eBay.com online auction site and posts a message on its web home page using the present invention. and then leaves the web site. A user Y goes to eBay.com and sees user X's message if X's user profile data meets Y's acceptance criteria data and if user Y's message criteria data matches to user X's posted message's message profile data. Alternatively, a two-way match process is used. User Y sees user X's message if X and Y form a two-way match of user profile data to acceptance criteria data and if user Y's message profile criteria data matches to user X's posted message's message profile data.

In another alternative, user Y may see all messages, with an indication associated with each message about the degree of match between Y and the user who posted the message. Or the user may be provided a threshold control for selecting the minimum match score of messages to be displayed.

To summarize the web surfing community forums embodiment, let's take an example. A single forum, called "web surfers," is created by Local2Me.com to dynamically match web surfers from all over the world as they are surfing web sites. It allows users to chat with each other in a group forum when they are on the same web site. A user John joins the web surfers forum through the Local2Me.com web site. He sets his user profile as a 23 year old single male, living in New York City. He sets his user profile acceptance criteria data to match men and women between ages of 18–28, within 100 miles of him. A separate window for chatting opens next to his main browser window. John now begins surfing the web in his main browser window, and as he enters each web site, the chatting window updates to show him the users also browsing that web site that he's matched to. John can now exchange messages with users as he surfs the web.

Clearly, in the burgeoning online communications arena there will be other electronic forums that can apply the present invention to great avail.

CONCLUSION, RAMIFICATIONS, AND SCOPE OF INVENTION

Thus the reader will see that the present invention, Dynamically Matching Users for Group Communication, provides a process by which individuals of all ages and profiles may locate very high quality, personalized matched groups of people for highly satisfying affinity group communications and community.

While my above description contains many specificities, these should not be construed as limitations on the scope of the invention, but rather as an exemplification of one preferred embodiment thereof. Many other variations are possible. Several examples, including newsgroups, online chat, web discussion boards, and instant messaging have been explored in the alternative embodiments section above.

Accordingly the scope of the invention should be determined not by the embodiment(s) illustrated, but by the appended claims and their legal equivalents.

What is claimed is:

1. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics;

b) obtaining acceptance criteria data and user profile data corresponding to the acceptance criteria parameters and user profile data parameters for each user of a multiplicity of users;

c) calculating the degree of match between the user profile data of each user and the acceptance criteria data of all other users of said multiplicity of users, and using the results of those calculations that exceed a particular threshold level of match to identify a subgroup associated with each said user; and

d) upon receipt by the system of a communication from a particular one of said users including message data and user identity data, making said message data available to all other members of the subgroup associated with said particular one of said users.

2. A method of dynamically matching defined users of a group communication system, so that subgroups of the users

having certain characteristics can intercommunicate, comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics;

b) obtaining acceptance criteria data and user profile data corresponding to the acceptance criteria, parameters and user profile data parameters for each user of a multiplicity of users;

c) calculating the degree of match between the user profile data of each user and the acceptance criteria data of all other users of said multiplicity of users, and using the results of those calculations to identify a subgroup associated with each said user based on the degree of match having a particular relationship to a level of match threshold defined for all other users of said multiplicity of users; and

d) upon receipt by the system of a communication from a particular one of said users including message data and user identity data, said system makes said message data available to all members of the subgroup associated with said particular one of said users.

3. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics

b) obtaining acceptance criteria data and user profile data corresponding to the acceptance criteria parameters and user profile data parameters for each user of a multiplicity of users;

c) receiving a communication from a particular one of said multiplicity of users including message data and user identity data;

d) calculating the degree of match between the user profile data of said particular one user and the acceptance criteria data of each other user of said multiplicity of users, and using the results of those calculations, which have a particular relationship to a specific level of match threshold, to identify a subgroup associated with said particular one user; and

e) making said message data available to all members of said subgroup.

4. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics,

b) obtaining acceptance criteria data and user profile data corresponding to the acceptance criteria parameters and user profile data parameters for each user of a multiplicity of users;

c) receiving a communication from a particular one of said multiplicity of users including message data and user identity data;

d) calculating the degree of match between the user profile data of said particular one user and the acceptance criteria data of each other user of said multiplicity of users, and using the results of those calculations to identify a subgroup associated with said particular one user based on the degree of match having a particular relationship to a level of match threshold defined for each user of said multiplicity of users; and

e) making said message data available to all members of said subgroup.

5. A method of dynamically matching defined and unknown users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics;

b) obtaining, acceptance criteria data corresponding to the acceptance criteria parameters for each user of a multiplicity of users;

c) receiving a communication from an unknown user including message data and user profile data;

d) calculating the degree of match between the user profile data of said unknown user and the acceptance criteria data of each user of said multiplicity of users, and using the results of those calculations; which have a particular relationship to a specific level of matching threshold, to identify a subgroup associated with said unknown user; and

e) making said message data available to all members of said subgroup.

6. A method of dynamically matching defined and unknown users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics;

b) obtaining acceptance criteria data corresponding to the acceptance criteria parameters for each user of a multiplicity of users;

c) receiving a communication from an unknown user including message data and user profile data;

d) calculating the degree of match between the user profile data of said unknown user and the acceptance criteria data of each user of said multiplicity of users, and using the results of those calculations to identify a subgroup associated with said unknown user based on the degree of match having a particular relationship to a level of match threshold defined for each user of said multiplicity of users; and

e) making said message data available to all members of said subgroup.

7. A method of dynamically matching defined and unknown users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics;

b) receiving a communication from an unknown user including message data and user profile data;

c) obtaining acceptance criteria data corresponding to the acceptance criteria parameters for each user of a multiplicity of users;

d) calculating the degree of match between the user profile data of said unknown user and the acceptance criteria data of each user of said multiplicity of users, and using the results of those calculations, which have a particular relationship to a specific level of match threshold, to identify a subgroup associated with said unknown user; and

e) making said message data available to all members of said subgroup.

8. A method of dynamically matching defined and unknown users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics.

b) receiving a communication from an unknown user including message data and user profile data;

c) obtaining acceptance criteria data corresponding to the acceptance criteria parameters for each of a multiplicity of users;

d) calculating the degree of match between the user profile said unknown user and the acceptance criteria data of each user of said multiplicity of users, and using the results of those calculations to identify a subgroup associated with said unknown user based on the degree of match having a particular relationship to a level of match threshold defined for each user of said multiplicity of users; and

e) making said message data available to all members of said subgroup.

9. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics;

b) obtaining user profile data corresponding to the user profile data parameters for each user of a multiplicity of profiled users;

c) receiving a communication from a particular one of said multiplicity of profiled users including message data and user identity;

d) obtaining acceptance criteria data corresponding to the acceptance criteria parameters for each of a multiplicity of other users who may or may not be profiled users;

e) calculating the degree of match between the user profile data of said particular one user and the acceptance criteria data of said multiplicity of other users, and using the results of those calculations, which have a particular relationship to a specific level of match threshold, to identify a subgroup associated with said particular one user; and

f) making said message data available to all members of said subgroup.

10. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, comprising the steps of:

a) establishing acceptance criteria parameters and user profile data parameters defining said characteristics,

b) obtaining user profile data corresponding to the user profile data parameters for each user of a multiplicity of profiled users;

c) receiving a communication from a particular one of said multiplicity of profiled users including message data and user identity data;

d) obtaining acceptance criteria data corresponding to the acceptance criteria parameters for each user of a multiplicity of other users who may or may not be profiled users;

e) calculating the degree of match between the user profile data of said particular one user and the acceptance criteria data of each user of said multiplicity of other users, and using the results of those calculations to identify a subgroup associated with said particular one user based on the degree of match having a particular relationship to a level of match threshold defined for each user of said multiplicity of other users; and

f) making said message data available to all members of said subgroup.

11. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, as recited in any one of claims **1**, **2**, **3**, and **4** wherein in step b) acceptance criteria data and user profile data are obtained by extracting information from sources other than directly from the users.

12. A method of dynamically matching defined and unknown users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, recited in any one of claims **5**, **6**, **7**, and **8** wherein in said obtaining step acceptance criteria data is obtained by extracting information from sources other than directly from the users.

13. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, as recited in any one of claims **9** and **10** wherein in step d) acceptance criteria data is obtained by extracting information from sources other than directly from the users.

14. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate as recited in any one of claims **9** and **10** wherein in step b) user profile data is obtained by extracting information from sources other than directly from the users.

15. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, as recited in any one of claims **3** and **4** wherein in step d) the degree of match between the acceptance criteria data of said particular one user and the user profile data of each other user of said multiplicity of users is also included in the calculation of the degree of match.

16. A method of dynamically matching defined and unknown users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, as recited in any one of claims **5**, **6**, **7**, and **8** and further comprising the step of:

before said calculating step, obtaining user profile data corresponding to user profile data parameters for each user of said multiplicity of users;

wherein the communication received from said unknown user in said receiving step additionally includes acceptance criteria data; and

wherein in said calculating step the degree of match between acceptance criteria data of said unknown user and user profile data of each user of said multiplicity of users is also included in the calculation of the degree of match.

17. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate as recited in any one of claims **1** and **2** wherein in step c) the degree of match between acceptance criteria data of each said user to user profile data of all other users of said multiplicity of users is also included in the calculation of the degree of match.

18. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, as recited in any one of claims **9** and **10** and further comprising the steps of:

before said calculating step, collecting user profile data corresponding to user profile data parameters or ones of

said multiplicity of other users for whom user profile data is not known; and

collecting acceptance criteria data corresponding to acceptance criteria data parameters for said particular one user;

wherein in step e) the degree of match between the collected acceptance criteria data and the user profile data of said multiplicity of other users who are profiled users is also included in the calculation of the degree of match, and the degree of matches between the collected acceptance criteria data and the collected user profile data is also included in the calculation of the degree of match.

19. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, recited in any one of claims **9** and **10** and further comprising the step of:

before said calculating step, collecting user profile data corresponding to user profile data parameters for ones of said multiplicity of other users for whom user profile data is not known;

wherein in step c) additionally receiving acceptance criteria data corresponding to the acceptance criteria data parameters for said particular one;

wherein in step e) the degree of match between the acceptance criteria data of said particular one and the user profile data of said multiplicity of other users who are profiled users is also included in the calculation of the degree of matches, and the degree of match between the acceptance criteria data of said particular one and the collected user profile data is also included in the calculation of the degree of matches.

20. A method as recited in any one of claims **1–8** and further comprising the steps of:

associating a unique message identifier with said message data;

associating said subgroup with said unique message identifier;

receiving a reply communication from one user of said subgroup including reply message data, reply user identity data, and said unique message identifier; and

making said reply message data available to said subgroup.

21. A method of dynamically matching defined users of a group communication system, so that subgroups of the users having certain characteristics can intercommunicate, as recited in claim **2**

wherein in step d) an indication of degree of match to each member of said subgroup is also made available to all members of the subgroup associated with said particular one of said users.

22. A method as recited in any one of claim **4**, **6**, **8**, and **10**

wherein in sad making step an indication of degree of match to each member of said subgroup is also made available to all members of said subgroup.

* * * * *

US 20030065727A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0065727 A1

Clarke et al. (43) Pub. Date: Apr. 3, 2003

(54) SYSTEMS AND METHODS FOR PROVIDING SECURED ELECTRONIC MESSAGING

(75) Inventors: **Forrest James Clarke**, Richmond, VA (US); **Bradley Carl Zeigler**, Richmond, VA (US); **Abhik Sengupta**, Richmond, VA (US)

Correspondence Address:
Finnegan, Henderson, Farabow
Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, DC 20005-3315 (US)

(73) Assignee: **Capital One Financial Corporation**

(21) Appl. No.: **10/138,566**

(22) Filed: **May 6, 2002**

Related U.S. Application Data

(60) Provisional application No. 60/325,216, filed on Sep. 28, 2001.

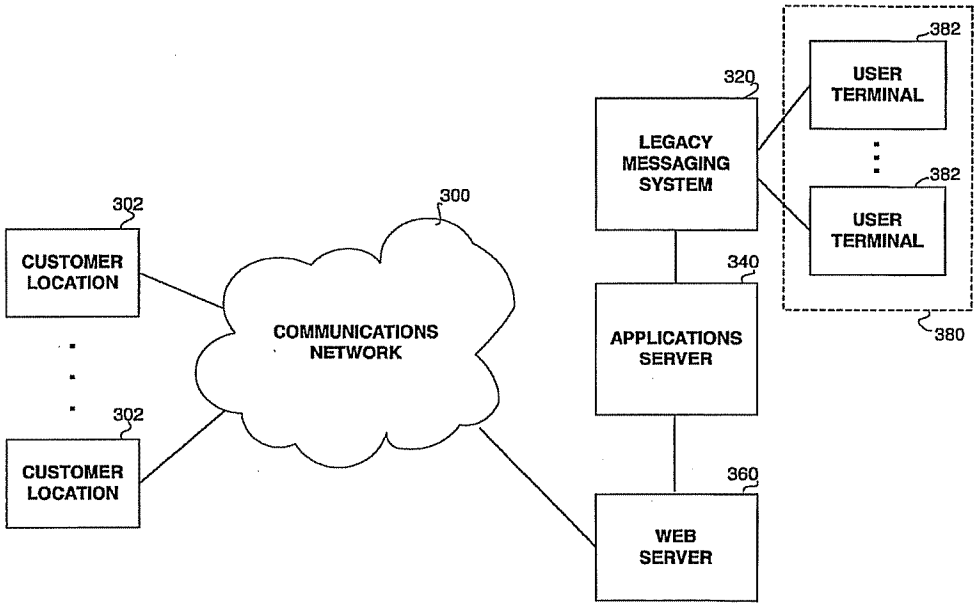
Publication Classification

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/206**; 709/246

(57) **ABSTRACT**

Systems and methods are disclosed for providing secured messaging in a communications network environment. The network environment may include public communication channels or networks, such as the Internet. Embodiments of the invention may be implemented to facilitate secured electronic messaging between any combination of entities, such as one or more customer locations and a message center. Further, consistent with embodiments of the invention, arrangements may be provided to permit the servicing of customers within a network environment that integrates legacy systems associated with a message center.



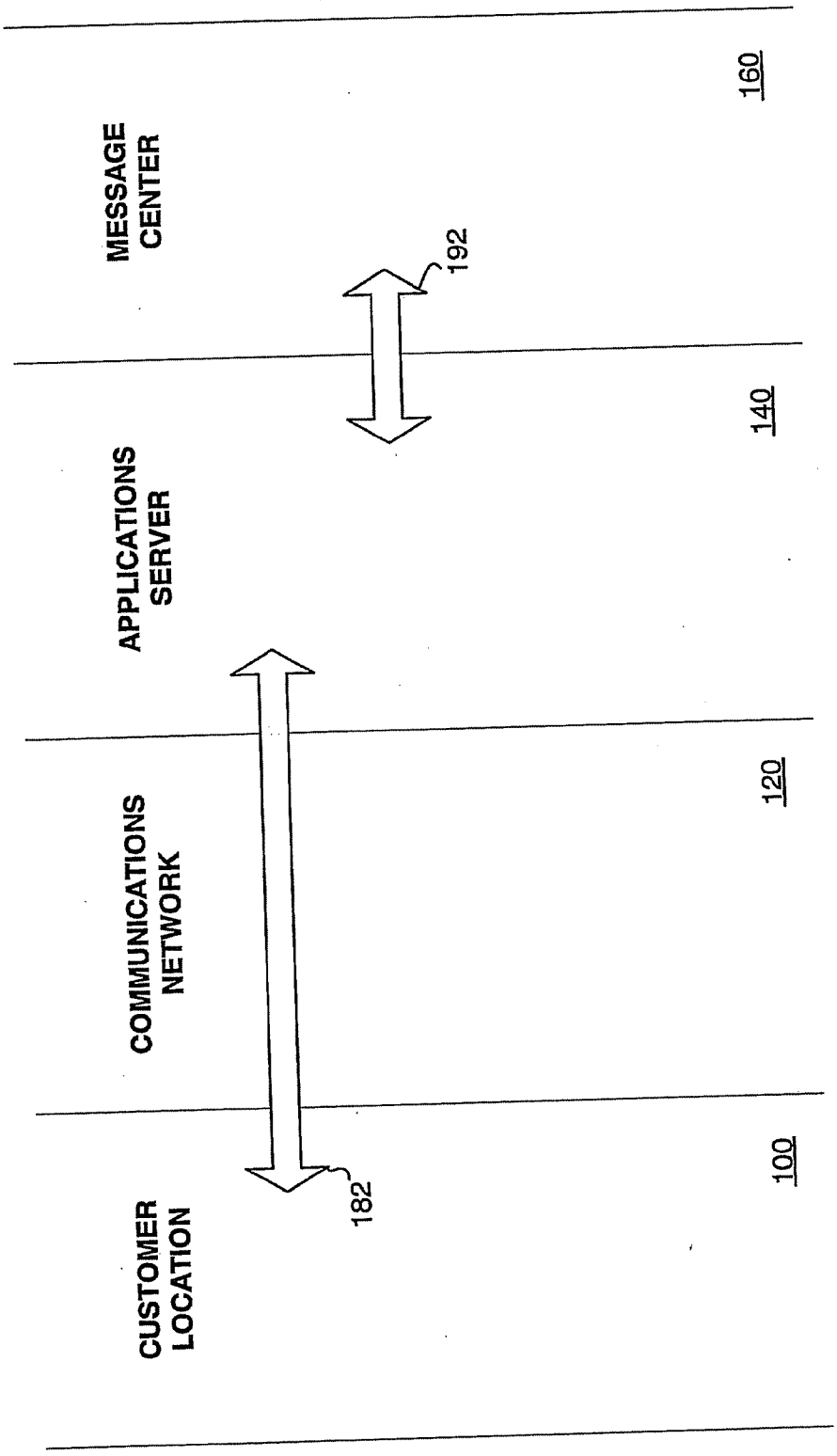
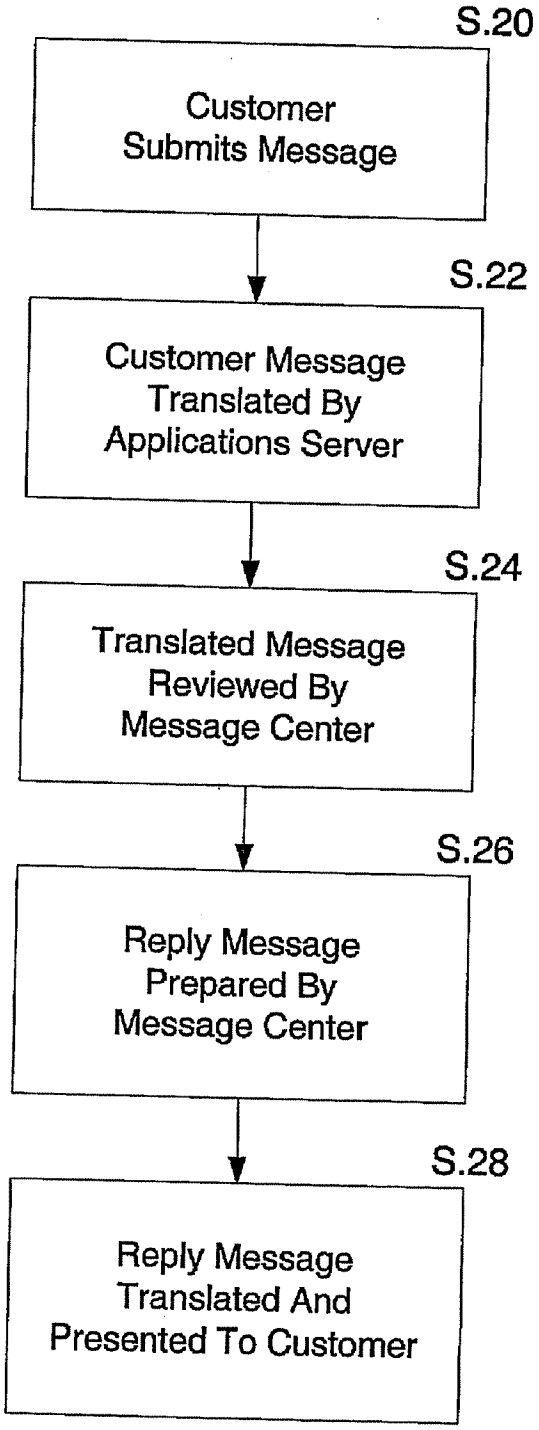

MESSAGE CENTER
160
192
APPLICATIONS SERVER
140
COMMUNICATIONS NETWORK
120
182
CUSTOMER LOCATION
100

FIG. 1

FIG. 2


S.20
Customer Submits Message
S.22
Customer Message Translated By Applications Server
S.24
Translated Message Reviewed By Message Center
S.26
Reply Message Prepared By Message Center
S.28
Reply Message Translated And Presented To Customer

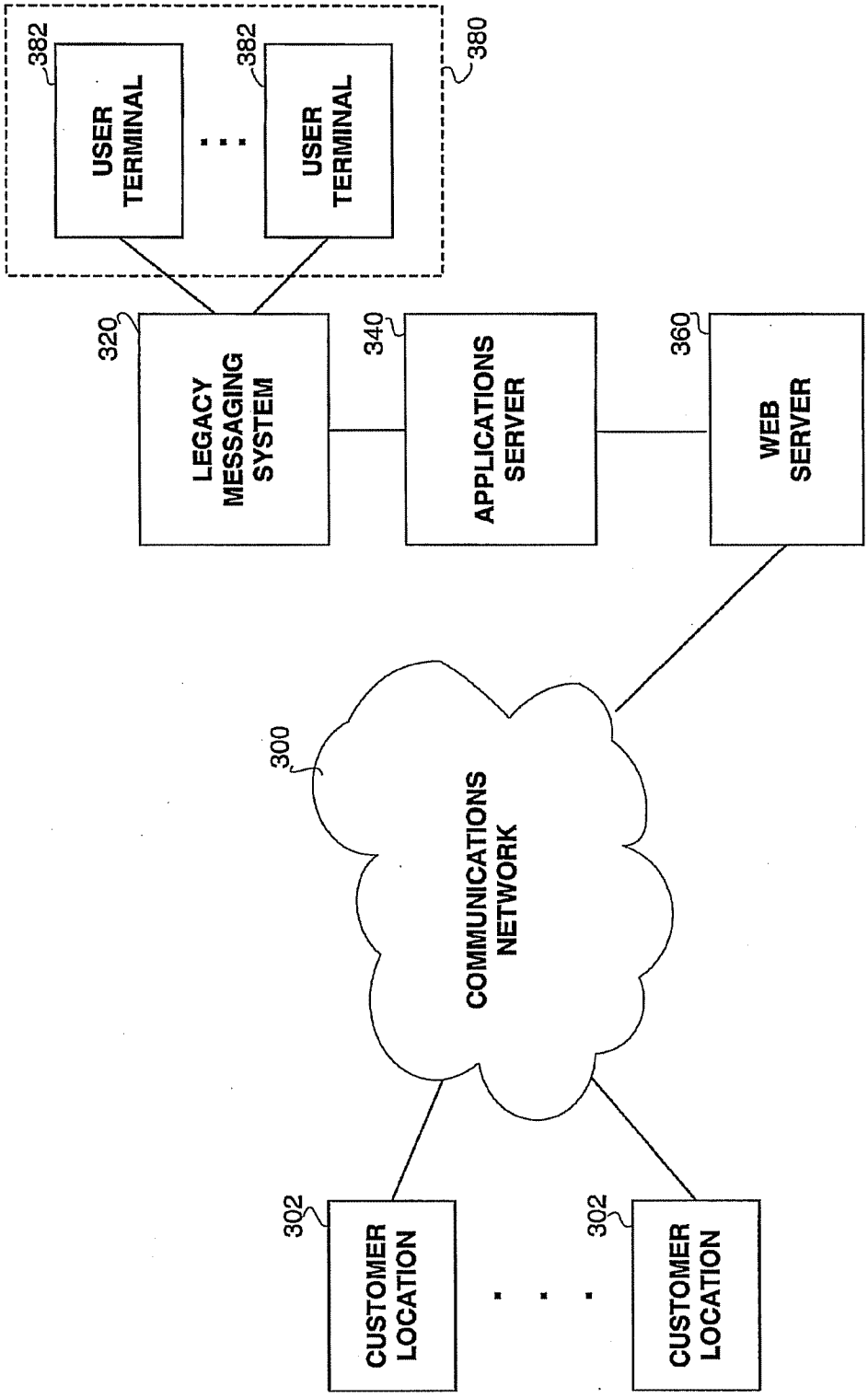
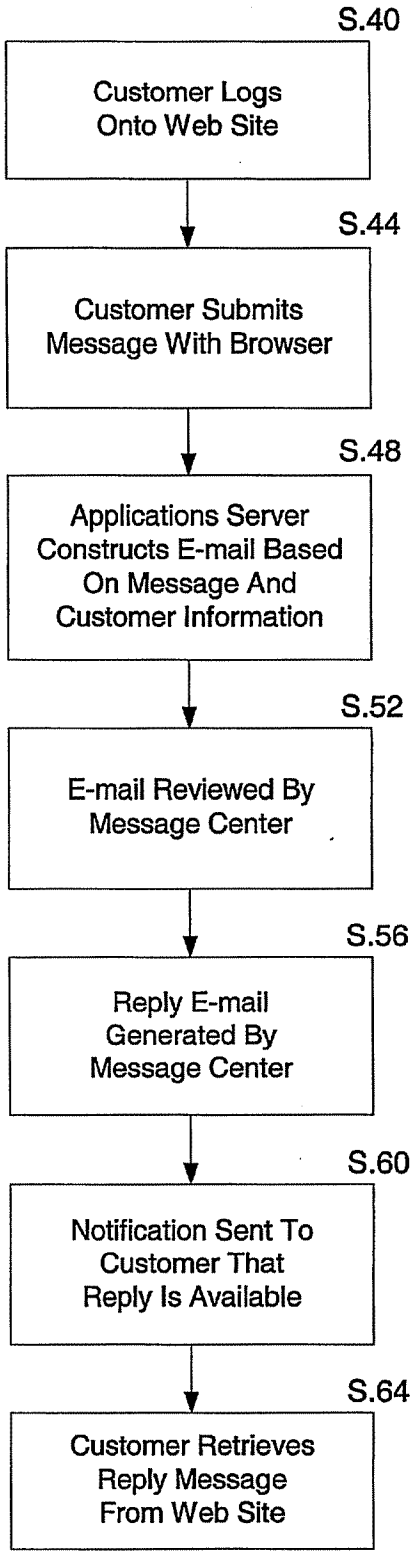

382
USER TERMINAL
382
USER TERMINAL
380
320
LEGACY MESSAGING SYSTEM
340
APPLICATIONS SERVER
360
WEB SERVER
300
COMMUNICATIONS NETWORK
302
CUSTOMER LOCATION
302
CUSTOMER LOCATION

FIG. 3

FIG. 4


S.40
Customer Logs Onto Web Site
S.44
Customer Submits Message With Browser
S.48
Applications Server Constructs E-mail Based On Message And Customer Information
S.52
E-mail Reviewed By Message Center
S.56
Reply E-mail Generated By Message Center
S.60
Notification Sent To Customer That Reply Is Available
S.64
Customer Retrieves Reply Message From Web Site

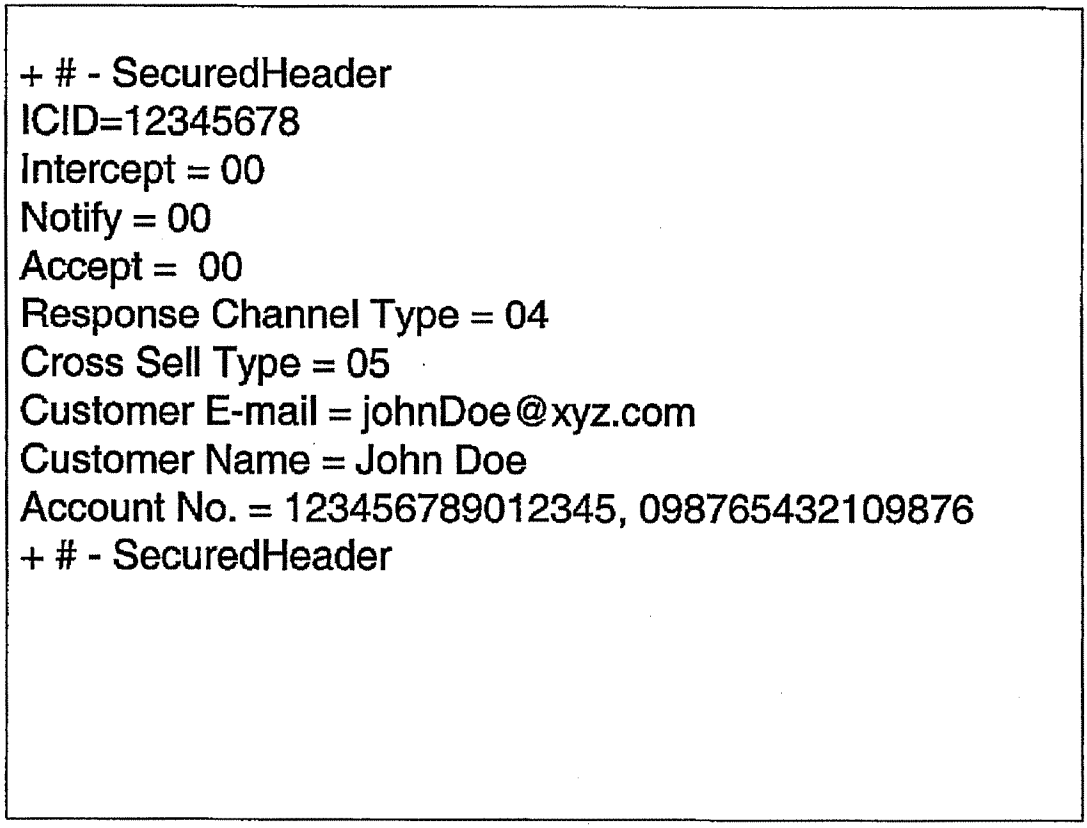

+ # - SecuredHeader
ICID=12345678
Intercept = 00
Notify = 00
Accept = 00
Response Channel Type = 04
Cross Sell Type = 05
Customer E-mail = johnDoe@xyz.com
Customer Name = John Doe
Account No. = 123456789012345, 098765432109876
+ # - SecuredHeader

FIG. 5

Dear Mr. Doe,

Here's the answer to your current question.
+ # - INTERCEPT = 01 - # +

We appreciate hearing from you.

Regards,
Company ABC

Original Message Follows:

+ # -
ICID=12345678
Intercept = 00
Notify = 00
Accept = 00
Customer E-mail = johnDoe@xyz.com
Customer Name = John Doe
Account No. = 123456789012345, 098765432109876
- # +

Dear Company ABC:

This is my question about my account.

Thank you for your prompt response.

John Doe

FIG. 6

Dear Mr. Doe,

Here's the answer to your current question.

We appreciate hearing from you.

Regards,
Company ABC

Original Message Follows:

Dear Company ABC:

This is my question about my account.

Thank you for your prompt response.

John Doe

FIG. 7

SYSTEMS AND METHODS FOR PROVIDING SECURED ELECTRONIC MESSAGING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority under 35 U.S.C. §119(e) to U.S. Provisional Application No. 60/325,216, filed on Sep. 28, 2001, the entire contents of which are incorporated by reference herein.

BACKGROUND OF THE INVENTION

[0002] I. Field of the Invention

[0003] The present invention relates to the fields of communications and electronic messaging. More particularly, the invention relates to systems and methods for providing secured electronic messaging in a communications network environment.

[0004] II. Background Information

[0005] To retain customers and improve sales, many businesses provide customer contact or message centers. Such message centers are staffed with customer agents or representatives to answer questions and provide assistance to customers. A customer message center may be implemented as a call center to permit customers to interact with representatives by telephone. In such cases, a toll-free number may be provided to access the call center by telephone and gather needed information (such as product or account information). Message centers may also permit customers to submit inquiries by written correspondence or mail. In certain cases, businesses may provide help desks or kiosks that are located at store location(s) or in shopping area(s) to directly service customers.

[0006] In today's technology-driven world, many customers expect fast and convenient assistance of their service needs from businesses. As a result, instead of using more traditional forms of communication (such as written correspondence or in-person contact), most customers prefer to use more modern technology and communication channels to access information. For example, modern voice communication channels, including wired and mobile phone systems, can provide flexibility and real-time access to information from customer service representatives. The Internet has also created new communications channels and, as a result, placed increasing demands on businesses to communicate and provide service to customers through e-mail and the Web.

[0007] Many businesses, including companies that have large customer segments, have invested in message centers that are capable of handling high call volumes on a daily basis. Despite such investments, customers are often required to wait extended periods of time on the phone before being connected with a customer service agent or before receiving any requested information. Some call centers incorporate automated, voice response equipment to process call traffic and provide easy access to frequently requested information. While such attempts have proven useful, they do not mitigate the majority of call traffic and, in certain cases, fail to provide the necessary support or information for customers.

[0008] As companies attempt to provide more efficient and personalized customer service, there is an increasing demand to handle higher volumes of requests by e-mail, the Web and other communication channels facilitated by the Internet. The Internet and the World Wide Web provide a global communications architecture that permits users to access information from Web sites and communicate using e-mail and other electronic communication or messaging techniques. As individuals become more accustomed to the Internet and electronic communication, the ability to adapt and use these communication channels will enable companies to successfully mitigate call traffic and provide service at a lower cost. There are, however, several existing challenges that face companies seeking to provide these new communication channels for customers.

[0009] For example, modern public communication networks, such as the public Internet, do not provide sufficient privacy or protection to permit confidential information to be transmitted to customers. Customers seeking confidential information, such as balance or credit information in relation to their financial account, must be supported with a communication channel or method that is secure to maintain privacy and confidentiality. Further, Web sites and customer databases are subject to attack and infiltration by unauthorized users or hackers. Therefore, additional measures must be taken to provide secure communication over public communications networks, especially when sensitive or confidential information needs to be stored and/or provided to customers.

[0010] Companies must also deal with integrating existing database and messaging systems to accommodate these more modern communication channels. While these existing systems may permit call center activity and internal e-mail routing, they are often limited or incompatible with modern technology (such as technology that permits communication through a Web site or public e-mail routing). Thus, companies are faced with either replacing their existing systems or finding a solution that will permit integration of newer technology, while still maintaining their investment in their existing customer contact systems.

[0011] Moreover, past attempts to provide e-business solutions and customer messaging by e-mail or other electronic messaging arrangements have not proven useful. For example, many e-business applications that permit customers to submit inquiries by e-mail or through a Web site are not compatible with legacy messaging systems. Further, past attempts are limited in their handling of customer messages and/or do not provide sufficient information to permit proper handling of customer messages by a message center.

SUMMARY OF THE INVENTION

[0012] In accordance with embodiments of the invention, systems and method are provided for facilitating secured messaging. Generally, such systems and methods provide secured messaging in a network environment that includes a public communications network, such as the Internet. Embodiments of the invention may be adapted to provide secured electronic messaging for facilitating communications between, for example, customers and a customer service or message center. Embodiments of the invention may also be adapted to provide secured messaging in network environments that incorporate legacy or existing systems.

[0013] Consistent with embodiments of the invention, a method is provided for secured messaging. The method

includes: receiving, over a first secured communications channel, a message from a customer at a customer location; translating the message from the customer location into an e-mail, the e-mail being addressed to an address that is accessible by a message center through a legacy messaging system; retrieving, at the message center, the e-mail through the legacy messaging system; preparing, at the message center, a reply e-mail that includes a response to the message from the customer location; retrieving, over a second secured communications channel, the reply e-mail from the legacy messaging system; and translating the reply e-mail into a message format that can be presented to the customer at the customer location.

[0014] Consistent with yet additional embodiments of the invention, a system is provided for secured messaging between a customer and a message center. The system includes: means for receiving a message from the customer at a customer location; means for translating the message from the customer location into an e-mail, the e-mail being addressed to a mailbox address that is accessible by the message center through a legacy messaging system; means for retrieving, at the message center, the e-mail through the legacy messaging system; means for preparing, at the message center, a reply e-mail that includes a response to the message from the customer location; means for retrieving, at an applications server, the reply e-mail from the legacy messaging system; and means for translating the reply e-mail into a message format that can be presented to the customer at the customer location.

[0015] Other embodiments of the invention provide a method for provide secure messaging between a plurality of customers and a message center. Such methods include: providing a Web site that is accessible over the Internet, the Web site including at least one message input screen; receiving, as part of a secure messaging session with a customer location, a message from a customer entered through the at least one message input screen; forwarding, as part of a secure Hypertext Transfer Protocol (HTTPS) request, the message of the customer to an applications server; constructing, at the applications server, an e-mail containing the message of the customer, the e-mail being addressed to a private mailbox address that is accessible by the message center; and examining, at the message center, the e-mail constructed by the applications server and generating a reply e-mail, the reply e-mail including a reply to the message of the customer.

[0016] Systems for providing secure messaging may also be implemented, consistent with the invention. Such systems may include: a Web server connected to a plurality of customer locations over a public communications network, the Web server being adapted to receive a message from a customer during a secure messaging session with one of the plurality of customer locations; an applications server connected to the Web server and adapted to receive the message from the customer during a secure messaging session with the Web server; and a private e-mail system connected to the applications server and a message center.

[0017] In response to the message from the customer, the applications server may be adapted to: construct an e-mail containing the message of the customer, the e-mail being addressed to a private mailbox address that is accessible by the message center through the private e-mail system; retrieve, through the private e-mail system, a reply e-mail generated by the message center, the reply e-mail including a reply to the message of the customer; and translate the reply e-mail into a message format that can be presented to the customer at the customer location.

[0018] Consistent with additional embodiments of the invention, systems may be provided for secure messaging. These systems may include: a Web server adapted to receive a message from a customer during a secure messaging session with a customer location; an applications server connected to the Web server and adapted to receive the message from the customer during a secure messaging session with the Web server; and a messaging system connected to the applications server and a message center.

[0019] In response to the message from the customer, the applications server may be adapted to: construct an e-mail containing the message of the customer, the e-mail including a data header with customer information and message handling information; forward the e-mail to an address that is accessible by the message center through the messaging system; retrieve, through the messaging system, a reply e-mail generated by the message center, the reply e-mail including a reply to the message of the customer; and translate the reply e-mail into a message format that can be presented to the customer at the customer location.

[0020] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only, and should not be deemed restrictive of the full scope of the invention, as claimed herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The accompanying drawings, which are incorporated herein and constitute a part of this specification, illustrate various features and aspects of embodiments of the invention. In the drawings:

[0022] **FIG. 1** illustrates an exemplary system environment for providing secured messaging, consistent with embodiments of the invention;

[0023] **FIG. 2** is an exemplary flowchart of a method for providing secured messaging, consistent with embodiments of the invention;

[0024] **FIG. 3** illustrates another exemplary system environment for providing secured messaging, consistent with embodiments of the invention;

[0025] **FIG. 4** is another exemplary flowchart for providing secured messaging, consistent with embodiments of the invention;

[0026] **FIG. 5** is an exemplary data header that may be included in an e-mail message constructed by an applications server, consistent with embodiments of the invention;

[0027] **FIG. 6** is an exemplary reply e-mail returned by a message center, consistent with embodiments of the invention; and

[0028] **FIG. 7** is an exemplary reply message presented to a customer, consistent with embodiments of the invention.

DETAILED DESCRIPTION

[0029] Embodiments of the present invention provide secured messaging in a communications network environ-

ment. The network environment may include public communication channels or networks, such as the Internet. Embodiments of the invention may be implemented to facilitate secured electronic messaging between any combination of entities, such as one or more customer locations and a message center. Consistent with embodiments of the invention, arrangements may be provided to permit the servicing of customers within a network environment that integrates legacy systems associated with a message center.

[0030] **FIG. 1** illustrates an exemplary system environment for providing secured messaging, consistent with embodiments of the invention. As illustrated in **FIG. 1, a** number of components may be provided, including a customer location **100**, a communications network **120**, an applications server **140** and a message center **160**. Although only one customer location **100** is illustrated in **FIG. 1**, any number of customer locations may be provided, with each customer location having access to or connectivity with communications network **120**. Further, while only one communications network **120**, one applications server **140**, and one message center **160** is illustrated in **FIG. 1**, these components can be provided in any number or quantity, depending on the needs and requirements of the system environment.

[0031] Each customer location **100** represents the location of a customer who communicates with message center **160** through communications network **120** and applications server **140**. As used herein, the term "customer" encompasses not only potential or actually customers of a company, but also partners, suppliers, clients, employees and other related entities of the company. Message center **160** may be staffed with customer service representatives or agents for the purposes of responding to messages from customers, providing information on products or services, and/or providing information concerning a customer's account (if applicable). Message center **160** may be provided for or operated by a company or business entity that provides goods or services to customers. For example, the company or business entity may be a financial institution that offers financial products or services to customers, such as savings accounts, checking accounts, credit card accounts, loans, investment services, accounting services and/or other types of financial products or services.

[0032] In **FIG. 1**, customer location **100** may include electronic communication equipment to access or connect to communications network **120**. By way of non-limiting examples, customer location **100** may include a personal computer, a workstation or a laptop computer that is configured with a modem or other communication hardware for establishing a dial-up or permanent connection with communications network **120**. Customer location **100** may also include a mobile or wireless phone, a personal digital assistant (PDA) or any other type of handheld device that is capable of establishing a wireless and/or wired connection with communications network **120**. Further, the communication equipment at each customer location **100** may include communication software and other applications (such as a browser application and/or e-mail software) to facilitate communications, messaging and/or accessing of information over communications network **120**.

[0033] Consistent with embodiments of the invention, communications network **120** may comprise any combination of technology and/or components for providing electronic communication with each customer location **100**. For electronic or on-line communication, communications network **120** may comprise any combination of wired or wireless technologies and/or communication networks, such as an intranet, the public Internet and/or a public switched telephone network (PSTN). Local-loop systems, gateway and/or service providers (such as Internet Service Providers (ISP)) may also be provided as part of communications network **120** to facilitate connectivity and/or communication services for each customer location **100**.

[0034] Applications server **140** is provided to receive, translate and/or coordinate messages between customer location **100** and message center **160**. Applications server **140** may be implemented with a server or computer-based platform and may include communication hardware and software. Software may also be provided with applications server **140** to provide one or more levels of security between communications network **120** and message center **160**, such as a company or private firewall. Alternatively, applications server **140** may be provided as part of a corporate or private network, that is isolated or secured from communications network **120** through a firewall. Additionally, applications server **140** may be provided with a database for storing customer information and message content information.

[0035] As indicated above, message center **160** may be staffed with customer service representatives or agents for the purposes of providing customer service features, such as responding to messages from customers, providing information, and performing other customer service functions. Message center **160** may include a number of components, such as user terminals that are operated by customer service agents. The user terminals may include computer-based workstations for accessing information requested by customers. Legacy messaging systems, which permit the sending and receiving of e-mail or other electronic messages, may also be provided as part of message center **160**. Legacy systems, such as a corporate or private e-mail system, may be accessible by applications server **140** and user terminals of message center **160** a over secure communications network or secure communication links to permit the sending and receiving of e-mail or other electronic messages. By way of a non-limiting example, legacy messaging systems may be provided as part of a corporate or private network along with message center **160** and/or applications server **140**. Consistent with embodiments of the invention, legacy messaging systems may also be hosted or implemented at separate location(s) from message center **160**, with connectivity between these systems being provided through a secure communication network or channel, such as a local area network or a virtual private network.

[0036] **FIG. 2** is an exemplary flowchart for providing secured messaging, consistent with embodiments of the invention. The features of **FIG. 2** may be used to facilitate secured messaging between any combination of entities, such as one or more customer locations and a message center. As illustrated in **FIG. 2**, the process begins with a customer submitting a message (step S.20). For example, a customer at customer location **100** may electronically submit a message using communications network **120**. The message may be directed to message center **160** and include any combination or number of questions and/or requests for information. The message from customer location **100** may

be electronically sent over communications network **120** and received by applications server **140** using a secure communications channel **182** (see **FIG. 1**). This secure communications channel may be provided in a number of different ways.

[0037] For example, if communications network **120** is implemented using the Internet, a Web site may be established to accept messages from customer location **100** and submit them to applications server **140**. For this purpose, a Web server may be provided separately or as part of communications network **120**, or could be implemented as part of applications server **140**. Such a Web server may host the Web site, which may be a company Web site or a Web site operated by a third party on-behalf of the company. The content of the Web site may be stored entirely or in part on the Web server and/or applications server **140**.

[0038] To provide security and restrict access, the Web site may require each customer to log-in or go through an authentication process before submitting a message. For example, a customer at customer location **100** may be required to provide authenticating information such as a valid password, account number and/or username or ID. Alternatively, the log-in or authentication process could be automated by, for example, using software that causes customer location **100** to automatically provide the necessary log-in or authentication information to the Web server. After successfully logging in, a message input screen may be displayed by the customer's browser. Using the message input screen, a customer may then submit a message or question from customer location **100** to the Web server.

[0039] Consistent with embodiments of the invention, one or more different message input screens may be presented to the customer depending on the type of question or information requested by the customer. For example, one message input screen may be provided to facilitate customers in requesting information concerning their account with a company, while other message input screens may be provided to facilitate customers in requesting general information concerning products or services of a company. A menu screen may also be provided to a customer to facilitate the selection and display of the proper message input screen(s). By using different message input screens, customer messages may be submitted and responded to more efficiently and with less errors or confusion.

[0040] Communication between the customer's browser and the Web server may follow a request/response paradigm involving Hypertext Transfer Protocol (HTTP). When an HTTP request is made by the browser (such as to view a Web page), the Web server provides a response (such as providing an HTML file to permit the Web page to be displayed by the browser). Thus, when a message input screen is completed by a customer, the content of the entered message may be sent as part of an HTTP request from the customer's browser. To transmit data between customer location **100** and the Web server, a secure messaging session may be established between the customer's browser and the Web server in accordance with a secure sockets layer protocol, such as HTTPS. Encrypted messages received from customer location **100** may be forwarded by the Web server to applications server **140**. If necessary, communication between the Web server and applications server **140** may also be established using HTTPS or another protocol providing sufficient security.

[0041] Other arrangements may be provided for establishing secure communications channel **182** between customer location **100** and applications server **140**. For example, a direct connection may be made between customer location **100** and applications server **140** over a PSTN or other public communications network. In such a case, customer location **100** can include applications software for dialing-up and connecting with applications server **140**, as well as performing authentication and message encryption routines. The application software may also generate one or more message input screens to facilitate the entry of messages or questions by a customer. Alternatively, customer messages may be submitted to applications server **140** using an e-mail system. For instance, customer location **100** may submit messages addressed to a mailbox accessible by applications server **140**. For this purpose, an e-mail server may be provided as part of communications network **120**. In addition, if a conventional, public e-mail system is used, then customer messages may be sent as an encrypted file attached to an e-mail. In such cases, various encryption techniques may be used, such as encryption algorithms based on public-private key arrangements.

[0042] Referring again to **FIG. 2**, after a message is submitted by customer location **100** (step S.20), the message is received and translated by applications server **140** (step S.22). Applications server **140** may perform one or more translation routines. For example, if the customer message is received in an encrypted form, applications server **140** may decrypt the message. Thereafter, applications server **140** may translate the message so that it may be accessed by message center **160**. For this purpose, applications server **140** may translate the message into a format that is accessible through an existing or legacy messaging center used by message center **160**. For example, if the legacy messaging system is a corporate or private e-mail system, then applications server **140** may generate an e-mail based on the customer's original message, with the e-mail being addressed to a mailbox address accessible by message center **160** through the private e-mail system.

[0043] The e-mail message generated by applications server **140** may incorporate the original message content submitted by the customer. Further, to facilitate proper handling of the customer's message, applications server **140** may incorporate other information into the e-mail message using, for example, data headers or character strings. The data headers or character strings may have a predefined format and can be included in any part of the e-mail message, such as the subject line or message field of the e-mail. The information incorporated by applications server **140** may include, for example, relevant customer information (such as a customer name or ID, and/or a customer account number). The customer information may be gathered based on information entered by the customer during an authentication process and/or may be collected from a customer database. Messaging handling information may also be includes using, for example, a message code or trigger in the subject line or message body of the e-mail. Such a message code or trigger may identify the type of message submitted by a customer (based on, for example, the type of message input screen used) and/or the priority level of the message (based on, for example, the status of the customer, the date of the original message, the type of message submitted by the customer, etc.). Consistent with embodiments of the invention, customer information and

message handling information may also be provided in a file (such as a text file) that is sent as an attachment with the e-mail generated by applications server **140**.

[0044] Each of translated message is then reviewed by message center **160** (step S.24). To retrieve and review a customer message, a secure communications channel **192** (see **FIG. 1**) is established between applications server **140** and message center **160**. Secure communications channel **192** may be implemented in a number of different ways. For example, the translated customer message may be sent by applications server **140** to a legacy messaging system using a secure, private or local area network or a virtual private network. The legacy messaging system, such as a corporate or private e-mail system, may be provided as part of message center **160** or provided at a separate location. A corporate or private e-mail system may be an internal e-mail system that is generally not accessible to the public or through public communications networks. Customer service representatives of message center **160** may access the legacy messaging system to retrieve and review the customer message using a dedicated, internal communication link or a secure, local area network. Alternatively, applications server **140** may forward the translated customer messages directly to the existing messaging system or customer agent workstations of message center **160** using a secure, dial-up or permanent communication link.

[0045] Customer service representatives may poll or review customer messages on a periodic basis. If customer information is provided with a customer message, then the customer information may be used by the customer service representatives to access information (such as customer account information) and/or determine an appropriate reply to the customer message. Further, if a message code or trigger is provided with a customer message, then the message code or trigger may be interpreted by the customer service agent to determine how to respond to the message. In addition, based on the specific nature of the customer's inquiry or the reply from the message center, a customer service representative may determine to update or change the message code or trigger. In any event, each of the translated customer messages from applications server **140** may be reviewed and replied to by message center **160**. As part of this process, a reply message is prepared by message center **160** (step S.26).

[0046] Consistent with embodiments of the invention, reply messages may be prepared by message center **160** using one or more legacy messaging systems. For example, customer service representatives may prepare a reply message to a customer using an existing corporate or private e-mail system. The reply message may include, for example, information requested by a customer and/or an answer to a question submitted by a customer. Information or answers provided in the reply message may contain confidential and/or non-confidential information. In addition, the customer's original message may be included as part of the reply message, as well as the relevant customer information (such as a customer name or ID, and/or a customer account number).

[0047] Reply messages generated by message center **160** may be forwarded to or retrieved by applications server **140**. For example, using secure communications channel **192** (see **FIG. 1**), reply messages may be forwarded to or retrieved by applications server **140**. In such cases, a customer service representative may send a reply message using the existing messaging system associated with message center **160**. The reply message may be addressed to a mailbox address accessible by applications server **140**. Applications server **140** may retrieve reply messages from the legacy messaging system through, for example, a secure, dial-up or permanent communication link, a private network or a virtual private network. Alternatively, the legacy messaging system may forward the reply message directly to applications server **140** using a secure, dial-up or permanent communication link or virtual private network.

[0048] Reply messages from message center **160** are translated by applications server **140** into a message format that can be presented to individual customers (step S.28). Reply messages may be translated in a number of different ways. For example, if customers are permitted to view reply message through a Web site, then applications server **160** may construct an HTML file to present the content of the reply message as part of a display screen generated by the customer's browser. Each HTML file may be indexed and stored in a database of applications server **140** according to customer identification information (customer name or ID, and/or customer account number). As part of step S.28, applications server **140** may generate an e-mail or post a message at a Web site to notify the customer that a reply from message center **160** is available. The customer at customer location **100** may then log on the Web site (if the customer is not already authenticated on the Web site) and request to view the reply message. In response to the request, applications server **140** may retrieve and forward the HTML file containing the content of the reply message to the Web server, which in turn would forward the HTML file to customer location **100**. Using the HTML file, the customer's browser would display the reply message content to the customer. To provide security, a secure messaging session may be established between customer location **100** and the Web server using a protocol such as HTTPS. As indicated above, HTTPS or another suitable protocol may also be used to transfer files between the Web server and applications server **140**.

[0049] If message triggers or codes are provided in the reply e-mail, then applications server **140** may review and remove the message handling information from the reply provided to the customer. The message handling information may examined by applications server **140** to determine the final values for the trigger or codes (for example, if updates were made by the message center) and, thus, the proper handling for the reply. For example, message trigger or code values may indicate the method by which the customer is to be notified and/or presented with the reply from the message center.

[0050] In addition to using the Web, other arrangements for providing the reply message to the customer may be used depending on the type of secure communications channel **182** established between customer location **100** and applications server **140**. For example, if a direct connection is made between customer location **100** and applications server **140** over a PSTN or another type of public communications network, then the reply message may be encrypted by applications server **140** and sent in a file format (such a text file) that may be opened and viewed by customer location **100**. Alternatively, reply messages may be forwarded by

applications server **140** using an e-mail system. For instance, applications server **140** may send the reply message to a mailbox accessible by customer location **100**. If a conventional, public e-mail system is used, then the reply message may be sent by applications server **140** as an encrypted file attached to an e-mail addressed to the customer.

[**0051**] As indicated above, embodiments of the invention provide secured messaging in a communications network environment, such as the Internet. Systems and methods consistent with the embodiments of the invention may be implemented to facilitate messaging of both confidential and non-confidential information. Such systems and methods may also be adapted to permit a message center to provide customer service in an environment that integrates legacy messaging systems of a message center.

[**0052**] Referring now to **FIG. 3**, another exemplary system environment is illustrated, consistent with embodiments of the invention. The exemplary system environment of **FIG. 3** may be adapted for use by a company that provides customer service features to its customers. For purposes of illustration, the exemplary system environment of **FIG. 3** and the related, exemplary method of **FIG. 4** will be described with reference to a financial company that provides financial products or services to customers, such as credit card accounts. It will be appreciated, however, that the examples of **FIGS. 3 and 4** may be adapted for use by customers of other products or services, as well as different types of companies that offer customer service features.

[**0053**] As illustrated in **FIG. 3, a** number of components may be provided in the exemplary system environment. For example, the system environment may include one or more customer locations **302**, a communications network **300**, a Web server **360**, an applications server **340**, a legacy messaging system **320** and a message center **380**. Although two customer locations **302** are illustrated in **FIG. 3**, any number of customer locations may be provided, with each customer location having access to or connectivity with communications network **300**. Further, while one communications network **300**, one Web server **360**, one applications server **340**, one legacy messaging system **320** and one message center **380** is illustrated in **FIG. 3**, these components may be provided in any number or quantity, depending on the needs and requirements of the system environment.

[**0054**] Similar to customer locations **100** of FIG.1, each customer location **302** of **FIG. 3** represents the location of a customer who communicates with message center **380** through communications network **300**. In the exemplary system environment of **FIG. 3**, the term "customer" encompasses not only potential or actually customers of a company, but also partners, suppliers, clients, employees and other related entities of the company. Message center **380** includes one or more user terminals **382** that are staffed with customer service representatives or agents for the purposes of responding to messages from customers, providing information on products or services, and/or providing information concerning a customer's account (if applicable). By way of a non-limiting example, message center **380** may be provided for or operated by a financial company or business entity that provides financial products or services to customers. For example, the financial company or business may provide one or more different types of credit card accounts to customers.

[**0055**] To access or connect to communications network **300**, customer location **302** may include suitable communication equipment. By way of non-limiting examples, customer location **302** may include a personal computer, a workstation or a laptop computer that is configured with a modem or other communication hardware for establishing a dial-up or permanent connection with communications network **300**. Customer location **302** may also include a mobile or wireless phone, a personal digital assistant (PDA) or any other type of handheld device that is capable of establishing a wireless and/or wired connection with communications network **300**. Further, the communication equipment at each customer location **302** may include communication software and other applications (such as a browser application and/or e-mail software) to facilitate communications, messaging and/or accessing of information over communications network **300**.

[**0056**] Communications network **300** facilitates communication between client locations **302** and the other system components of **FIG. 3**. For this purpose, communications network **300** may include any combination of technology and/or components for providing electronic communication. For example, communications network **300** may comprise any combination of wired or wireless technologies and/or communication networks, such as an intranet, the public Internet and/or a public switched telephone network (PSTN). Local-loop systems, gateway and/or service providers (such as Internet Service Providers (ISPs)) may also be provided as part of communications network **300** to facilitate connectivity and/or communication services for each customer location **302**.

[**0057**] Web server **360** hosts one or more Web sites that are accessible to customer locations **302**. Each Web site may be a company Web site, or a Web site that is operated by a third party on behalf of the company. The Web site may include a secure messaging portal or center for customers of the company to submit and receive messages. The content of each Web site may be stored entirely or in part on the Web server **360** and/or applications server **340**. As further described below, a Web site may be provided to facilitate the submission of messages by customer locations **302** and the retrieval of reply messages from message center **380**. Although **FIG. 3** illustrates Web server **360** as being connected to communications network **300**, Web server **360** may actually form part of the infrastructure for communications network **300**.

[**0058**] Applications server **340** facilitates integration of legacy messaging system **320**. Applications server **340** may be implemented with a server or computer-based platform and may include communication hardware and software. Software may also be provided with applications server **340** to perform message handling and routing functions, such as those described below in connection with **FIG. 4**. In addition, applications server **340** may include software to provide one or more levels of security between communications network **300** and message center **380**, such as a company or private firewall. Alternatively, applications server **340** may be provided as part of a corporate or private network, that is isolated or secured from communications network **300** through a firewall. Additionally, applications server **340** may also be provided with a database for storing customer information (such as customer name, account number(s), e-mail address, etc.) and message information.

[0059] The exemplary system environment of **FIG. 3** may include one or more legacy messaging systems **320**. By way of a non-limiting example, legacy messaging system **320** may be a corporate or private e-mail system or other type of electronic messaging system. The corporate or private e-mail system may be an internal e-mail system that is part of a corporate or private network and generally not accessible to the public or through public communications networks. Alternatively, the corporate or private e-mail system may be hosted externally, with access to the system being provided through a secured communication link or network, such as a virtual private network. The corporate or private e-mail system may incorporate functions to facilitate message tracking, categorization and handling by message center **380**. Examples of commercially available e-mail or messaging systems include Kana Response, available from Kana Communications, Inc. of Redwood City, Calif.

[0060] As illustrated in **FIG. 3**, message center **380** may include one or more user terminals **382**. User terminals **382** may be staffed with customer service representatives or agents for providing customer service features, such as responding to messages from customers, providing information, and performing other customer service functions. Each of the user terminals **382** may include computer-based workstations or terminals for sending and/or receiving messages through legacy messaging system **320**. User terminals **382** may also be connected to a corporate database server for accessing and retrieving information requested by customers. Connectivity between user terminals **382** and legacy messaging system **320** and the corporate database server may be provided through a secure, direct communication link or private communication network, such as a local area network.

[0061] **FIG. 4** illustrates an exemplary flowchart for providing secured messaging, consistent with embodiments of the invention. The features of **FIG. 4** may be used to facilitate secured messaging between entities in the exemplary system environment of **FIG. 3**, such as customer locations **302** and message center **380**. The exemplary process of **FIG. 4** begins with a customer logging onto a Web site (step S.40). As indicated above, the Web site may be established by a company to accept and handle messages from customer locations **302**. The Web site may be hosted by Web server **360**, with the content of the Web site being stored entirely or in part on Web server **360** and/or applications server **340**.

[0062] Using a browser, each customer location **302** may connect to the Web site through communications network **300**. Once connected to the Web site, a customer may be required to log-in or go through an authentication process before being able to submit messages to message center **380**. For example, customer location **302** may be required to provide authenticating information such as a valid password, account number and/or username or ID. Alternatively, the log-in or authentication process could be automated by, for example, using software that causes customer location **100** to automatically provide the necessary log-in or authentication information to the Web server.

[0063] After logging on to the Web site, the authenticated customer may then submit a message using the browser at customer location **302** (step S.44). The message include any combination or number of questions and/or requests for information. To facilitate the entry of messages, a message input screen may be generated by the customer's browser. For this purpose, an HTML file for generating a message input screen may be provided by Web server **360** to customer location **302**. A generic message input screen may be provided for all messages submitted by a customer. The generic input screen may include a subject select field to permit the customer to indicate the nature of his/her inquiry, and a comment field to enter the content of the message. Alternatively, depending on the type of question or information requested by the customer, specific message input screens may be generated by the customer's browser. For example, one message input screen may be provided to facilitate the customer in requesting information concerning their credit card account, while other message input screens may be provided to facilitate the customer in requesting general information concerning financial products or services of the company. If different message input screens are available, a menu screen may be displayed to the customer to facilitate the ultimate selection and display of the proper message input screen(s) by the customer's browser.

[0064] Once the message input screen is completed, the customer may submit the message (for example, by selecting a SEND or SUBMIT button). As part of this process, the information entered through the message input screen may be sent as part of an HTTP request from the customer's browser to Web server **360**. To transmit the message information between customer location **302** and Web server **360** in a secured fashion, a secure messaging session may be established between the customer's browser and Web server **360** in accordance with a secure sockets layer protocol, such as HTTPS. Web server **360** may forward the HTTP request to applications server **340** for further processing. If necessary, communication between Web server **360** and applications server **340** may also be established using HTTPS or another protocol providing sufficient security.

[0065] Referring again to **FIG. 4**, after the message information is submitted by customer location **302** (step S.44), applications server **340** may generate an e-mail for message center **380** based on the message information and relevant customer information (step S.48). For example, the subject field for the e-mail may be populated with the message type or subject selected by the customer. Further, the "to" address for the e-mail may be a mailbox address of message center **380** that is accessible through legacy messaging system **320**. The "from" address for the e-mail may be the customer's username or Web ID (such as an on-line Web servicing ID) with a domain associated with applications server **340**. The body of the e-mail may contain the message content or text information entered by the customer. The body of the e-mail may also include data or message headers to facilitate handling of the e-mail.

[0066] **FIG. 5** illustrates an exemplary data header that may be included in the e-mail messages constructed by applications server **340**. As illustrated in **FIG. 5**, the data header includes a character string ("+#–SecuredHeader") that initializes and closes the data header. The data header may include information that are used by customer service representatives at message center **380** in order to determine how to handle and/or respond to the customer's message. This information may include customer information (such as an Internet customer ID (ICID), a customer's name, customer account number(s), a customer's personal e-mail

address, etc.), as well as marketing or response information (such as Response Channel Type, Cross Sell Type, etc.). Relevant customer information may be gathered based on the information provided by a customer during an authentication process and/or accessed from a customer database. Marketing or response information may be incorporated into the e-mail by application server **340** based on numerous factors, such as the type of inquiry or message submitted by the customer, the status of the customer, the type of products or services requested by the customer, etc.

[0067] As further described below, the data header may also include message triggers (such as Intercept, Notify, Accept) which are set to initial values by applications server **340** to indicate handling instructions for the customer's message. These message triggers may be changed or updated to different values when the message is reviewed at message center **380**. For example, a customer service representative may determine that an initial value of a message trigger is improper based on the type of message or reply to be provided to the customer and may update the message trigger value to provide proper notification and/or handling of the reply for the customer.

[0068] After constructing the e-mail message, applications server **340** will forward the e-mail to legacy messaging system **320**. A secure, direct communication link or private network (such as a local area network) may be used to forward the e-mail from applications server **340** to legacy messaging system **320**. The e-mail may be sent to a general mailbox address for message center **380**. Alternatively, alias addresses may be defined for different categories of messages. Alias addresses may be formed from a combination of a codeword representing the message input screen type or subject selected by the customer and a domain associated with message center **320**. Consistent with embodiments of the invention, a set of alias addresses may be defined for customer's messages related to confidential information (such as questions related to a customer's credit card account) as well as customer's messages related to non-confidential information (such as an inquiry for application information for a financial product or service of the company, or a request concerning job openings with the company). The use of alias addresses may permit e-mails received by legacy messaging system **320** to be routed to the appropriate group or set of customer service representatives at message center **380**.

[0069] Referring again to **FIG. 4**, e-mails constructed by applications server **340** are reviewed by message center **380** (step S.52). To retrieve and review a customer message, a secure communications channel is established between applications server **340** and message center **380**. For example, communication between each of the user terminals **382** and legacy messaging system **320** may be established using a secure, direct communication link or a private network, such as local area network. With such a secure communications channel, customer service representatives at message center **380** may access legacy messaging system **320** through user terminals **382** to retrieve and review e-mails containing a customer's original message.

[0070] When reviewing an e-mail, a customer service representative may examine the content of the customer's original message to determine the nature of the inquiry. The customer service representative may also inspect the data header created by applications server **340** to identify the customer, access customer account information and/or determine how the message should be handled. As indicated above, message triggers can also be included in the data header with values initialized by applications server **340**. Such message triggers may be used to categorize the customer's message and/or provide message handling instructions. By way of non-limiting examples, message triggers and associated trigger values may be defined as follows:

[0071] INTERCEPT—Determines whether or not the customer will be notified of a reply message at the time of authentication into the Web site. If this value is required, the customer is required to read the reply message in order to proceed to other pages in the Web site. Exemplary INTERCEPT values: 0=none; 1=suggested intercept; and 2=required intercept.

[0072] NOTIFY—Indicates whether or not a notification message will be sent to the customer's personal e-mail address to indicate that a reply message is available. Exemplary NOTIFY values: 0=no notification; 1=send notification e-mail to customer.

[0073] ACCEPT—Specifies whether or not an Acceptance of Terms prompt will be presented to the customer following the review of the message. Exemplary ACCEPT values: 0=no acceptance of prompt required; 1=acceptance of terms prompt required.

[0074] After each e-mail is reviewed at message center **380**, a customer service representative will formulate a response and generate a reply e-mail (step S.56). The reply e-mail is forwarded by message center **380** to legacy messaging system **320** using a mailbox address that is accessible by applications server **340**. **FIG. 6** illustrates an exemplary reply e-mail, consistent with embodiments of the invention. As illustrated in **FIG. 6**, the reply e-mail may include the original message from the customer, as well as a message header that contains the reply message from a customer service representative. The data header created by applications server **340** is also maintained in the reply e-mail. However, the initial values of the message triggers may change based on new data headers added to the reply. This may occur if the customer service representative decides to change or update the value or uses a message template which includes a message header with a predefined trigger value. In the exemplary reply e-mail of **FIG. 6, a** message header is used with a INTERCEPT trigger. This trigger will set the value for INTERCEPT to "01" when the reply e-mail is processed by applications server **340**.

[0075] Each reply e-mail sent to legacy messaging system **320** is retrieved and processed by applications server **340**. To determine the proper handling for the reply, applications server **340** may parse the message trigger values in the data headers by scanning the reply e-mail from top to bottom. The first instance of each trigger may be used by applications server **340** to set the trigger value. After parsing, applications server **340** will strip or remove all data headers from the text body of the reply e-mail, and prepare an HTML file so that the reply message can be presented to the customer through the Web. Alternatively, if the original message and reply relate to non-confidential information, an e-mail may be constructed from the reply message and sent to a personal e-mail address of the customer.

[0076] After the reply e-mail is processed by applications server **340**, notification is sent to the customer that a reply

is available (step S.60). As indicated above, message triggers may be provided to indicate how notification is sent to the customer by applications server **340**. Thus, for example, the set trigger values may indicate that notification be sent to the customer's personal e-mail address. Alternatively, the set trigger values may indicate that notification be presented to the customer the next time the customer logs in and is authenticated through the Web site.

[0077] After receiving notification, the customer at customer location **302** may log on the Web site (if the customer is not already logged and authenticated on the Web site) and retrieve the reply message (step S.64). As part of this process, applications server **340** may retrieve and forward the HTML file containing the content of the reply message to Web server **360**. In turn, Web server **360** forwards the HTML file to customer location **302** and, using the HTML file, the customer's browser can display the reply message.

[0078] By way of a non-limiting example, **FIG. 7** illustrates an exemplary reply message that may be displayed with a customer's browser. As shown in the **FIG. 7**, the reply message text from the customer service representative and the customer's original message may be displayed to the customer. All data headers are removed and do not appear in the reply message.

[0079] To provide security, a secure messaging session may be established between customer location **302** and Web server **360** when an HTML file containing the reply message is forwarded to the customer location. For this purpose, a protocol such as HTTPS may be used to establish a secure messaging session. HTTPS or another suitable protocol may also be used to transfer HTML files between Web server **360** and applications server **340**.

[0080] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. For example, the pre-existing or legacy messaging system may incorporate templates that can be used by customer service representatives to construct a reply message to customers. Alternatively, reply messages from service representatives may be composed using free form text entered using the legacy messaging system.

[0081] In addition, the invention is not limited to the particulars of the embodiments disclosed herein. For example, the individual features of each of the disclosed embodiments may be combined or added to the features of other embodiments. In addition, the steps of the disclosed methods herein may be combined or modified without departing from the spirit of the invention claimed herein. For instance, messages may be received from both authenticated and non-authenticated customers. If a message is sent from an authenticated customer, it can be considered confidential with a reply message handled according to the secured messaging techniques disclosed herein. In contrast, non-confidential messages or messages received from non-authenticated customers may handled as general inquiries (such as from the public at large). In such cases, reply messages may be sent to a personal e-mail address of the entity that submitted the original message.

[0082] Accordingly, it is intended that the specification and embodiments disclosed herein be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

What is claimed is:

1. A method for providing secured messaging, the method comprising:

receiving, over a first secured communications channel, a message from a customer at a customer location;

translating the message from the customer location into an e-mail, the e-mail being addressed to an address that is accessible by a message center through a legacy messaging system;

retrieving, at the message center, the e-mail through the legacy messaging system;

preparing, at the message center, a reply e-mail that includes a response to the message from the customer location;

retrieving, over a second secured communications channel, the reply e-mail from the legacy messaging system; and

translating the reply e-mail into a message format that can be presented to the customer at the customer location.

2. A method according to claim 1, wherein the step of receiving the message from the customer comprises:

establishing a secure messaging session between the customer location and a Web server;

generating a message input screen at the customer location to permit entry of the message of the customer; and

transmitting a secure Hypertext Transfer Protocol (HTTPS) request from the customer location to the Web server, the HTTPS request including the message of the customer entered through the message input screen.

3. A method according to claim 2, wherein the step of receiving further comprises forwarding the HTTPS request from the Web server to an applications server.

4. A method according to claim 3, wherein the step of forwarding comprises establishing a secure messaging session between the Web server and the applications server using a secure sockets layer protocol.

5. A method according to claim 3, wherein the step of translating the message from the customer location comprises:

constructing, at the applications server, an e-mail addressed to the message center, the e-mail including customer information and at least one message trigger with an initial value; and

forwarding the e-mail addressed to the message center from the applications server to the legacy messaging system.

6. A method according to claim 5, further comprising:

examining, at the message center, each message trigger provided in the e-mail to determine if the initial value assigned to the message trigger is proper; and

updating, in the reply e-mail, the value of each message trigger if the initial value is determined to be improper.

7. A method according to claim 6, further comprising:

inspecting, at the applications server, the value of each message trigger; and

notifying, based on the value of each message trigger, the customer at the customer location that a reply from the message center is available.

8. A method according to claim 1, wherein the customer location includes a Web browser and further wherein the step of translating the reply e-mail comprises constructing an HTML file that can be interpreted by the Web browser at the customer location to display the response to the customer.

9. A method according to claim 1, further comprising:

notifying the customer at the customer location that a reply from the message center is available; and

forwarding, upon request from the customer, the reply e-mail in the message format that can be presented to the customer at the customer location.

10. A method according to claim 1, wherein the step of retrieving the reply e-mail comprises:

providing the second secured communications channel between the legacy messaing system and an applications server; and

forwarding the reply e-mail over the second secured communications channel from the legacy messaging system to the applications server.

11. A method according to claim 10, wherein the step of translating the reply e-mail comprises constructing an HTML file that can be interpreted by a Web browser at the customer location to display the response to the customer.

12. A system for providing secured messaging between a customer and a message center, the system comprising:

means for receiving a message from the customer at a customer location;

means for translating the message from the customer location into an e-mail, the e-mail being addressed to a mailbox address that is accessible by the message center through a legacy messaging system;

means for retrieving, at the message center, the e-mail through the legacy messaging system;

means for preparing, at the message center, a reply e-mail that includes a response to the message from the customer location;

means for retrieving, at an applications server, the reply e-mail from the legacy messaging system; and

means for translating the reply e-mail into a message format that can be presented to the customer at the customer location.

13. A system according to claim 12, wherein the means for receiving the message from the customer comprises:

means for establishing a secure messaging session between the customer location and a Web server;

means for generating a message input screen at the customer location to permit entry of the message of the customer; and

means for transmitting a secure Hypertext Transfer Protocol (HTTPS) request from the customer location to the Web server, the HTTPS request including the message of the customer entered through the message input screen.

14. A system according to claim 13, wherein the means for receiving the message from the customer further comprises means for forwarding the HTTPS request from the Web server to an applications server.

15. A system according to claim 14, wherein the means for forwarding the HTTP request comprises means for establishing a secure messaging session between the Web server and the applications server using a secure sockets layer protocol.

16. A system according to claim 14, wherein the means for translating the message from the customer comprises:

means for constructing, at the applications server, the e-mail addressed to the message center, the e-mail including customer information and at least one message trigger; and

means for forwarding the e-mail addressed to the message center from the applications server to the legacy messaging system.

17. A system according to claim 12, wherein the customer location includes a Web browser and further wherein the means of translating the reply e-mail comprises means for constructing an HTML file that can be interpreted by the Web browser at the customer location to display the response to the customer.

18. A system according to claim 12, further comprising:

means for notifying the customer at the customer location that a reply from the message center is available; and

means for forwarding, upon request from the customer, the reply e-mail in the message format that can be presented to the customer at the customer location.

19. A system according to claim 12, wherein the means for retrieving the reply e-mail comprises:

means for providing a secure communications channel between the legacy messaging system and an applications server; and

means for forwarding the reply e-mail over the secure communications channel from the legacy messaging system to the applications server.

20. A system according to claim 19, wherein the means for translating the reply e-mail comprises means for constructing an HTML file that can be interpreted by a Web browser at the customer location to display the response to the customer.

21. A method for provide secure messaging between a plurality of customers and a message center, comprising:

providing a Web site that is accessible over the Internet, the Web site including at least one message input screen;

receiving, as part of a secure messaging session with a customer location, a message from a customer entered through the at least one message input screen;

forwarding, as part of a secure Hypertext Transfer Protocol (HTTPS) request, the message of the customer to an applications server;

constructing, at the applications server, an e-mail containing the message of the customer, the e-mail being addressed to a private mailbox address that is accessible by the message center; and

examining, at the message center, the e-mail constructed by the applications server and generating a reply e-mail, the reply e-mail including a reply to the message of the customer.

22. A method according to claim 21, wherein the reply e-mail is addressed to a private mailbox that is accessible by the applications server.

23. A method according to claim 22, further comprising:

forwarding, over a secure communications channel, the reply e-mail from the message center to the applications server; and

generating, at the applications server, an HTML file based on the reply e-mail from the message center, the HTML file including the reply of the message of the customer.

24. A method according to claim 21, further comprising:

providing a private e-mail system that is accessible to the applications server and the message center.

25. A method according to claim 24, further comprising:

forwarding, from the applications server to the private e-mail system, the e-mail addressed to the private mailbox address of the message center; and

retrieving, at the message center, the e-mail from the private e-mail system.

26. A method according to claim 24, further comprising:

forwarding, from the message center to the private e-mail system, the reply e-mail addressed to the private mailbox address of the applications server; and

retrieving, at the applications server, the reply e-mail from the private e-mail system.

27. A method according to claim 21, further comprising:

constructing, at the applications server, an HTML file based on the reply e-mail from the message center; and

forwarding, as part of a secure messaging session with the customer location, the HTML file to a Web browser at the customer location to display the reply from the message center to the customer.

28. A method according to claim 21, further comprising:

forwarding, upon request from the customer, the reply e-mail in a message format that can be presented to the customer at the customer location.

29. A method according to claim 21, further comprising:

in response to the reply e-mail, notifying the customer at the customer location that the reply from the message center is available.

30. A system for providing secure messaging, the system comprising:

a Web server connected to a plurality of customer locations over a public communications network, the Web server being adapted to receive a message from a customer during a secure messaging session with one of the plurality of customer locations;

an applications server connected to the Web server and adapted to receive the message from the customer during a secure messaging session with the Web server; and

a private e-mail system connected to the applications server and a message center;

wherein, in response to the customer message received from the Web server, the applications server is adapted to:

construct an e-mail containing the message of the customer, the e-mail being addressed to a private mailbox address that is accessible by the message center through the private e-mail system;

retrieve, through the private e-mail system, a reply e-mail generated by the message center, the reply e-mail including a reply to the message of the customer; and

translate the reply e-mail into a message format that can be presented to the customer at the customer location.

31. A system according to claim 30, further comprising means for notifying the customer at the customer location that the reply from the message center is available.

32. A system according to claim 31, further comprising means for forwarding, upon request from the customer, the reply e-mail in a message format that can be presented to the customer at the customer location.

33. A system according to claim 30, wherein the applications server is adapted to translate the reply e-mail from the message center into an HTML file and further wherein the HTML file is forwarded by the Web server, as part of a secure messaging session with the customer location, to a Web browser at the customer location to display the reply from the message center to the customer.

34. A system for providing secure messaging, the system comprising:

a Web server adapted to receive a message from a customer during a secure messaging session with a customer location;

an applications server connected to the Web server and adapted to receive the message from the customer during a secure messaging session with the Web server; and

a messaging system connected to the applications server and a message center;

wherein, in response to the message from the customer, the applications server is adapted to:

construct an e-mail containing the message of the customer, the e-mail including a data header with customer information and message handling information;

forward the e-mail to an address that is accessible by the message center through the messaging system;

retrieve, through the messaging system, a reply e-mail generated by the message center, the reply e-mail including a reply to the message of the customer; and

translate the reply e-mail into a message format that can be presented to the customer at the customer location.

* * * * *

US006654779B1

(12) **United States Patent**
Tsuei

(10) **Patent No.: US 6,654,779 B1**
(45) **Date of Patent: Nov. 25, 2003**

(54) **SYSTEM AND METHOD FOR ELECTRONIC MAIL (E-MAIL) ADDRESS MANAGEMENT**

(75) Inventor: **Henry T. Tsuei**, Omaha, NE (US)

(73) Assignee: **First Data Resources**, Englewood, CO (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/291,367**

(22) Filed: **Apr. 14, 1999**

(51) **Int. Cl.**[7] **G06F 9/00**

(52) **U.S. Cl.** **709/101**; 709/206; 709/100

(58) **Field of Search** 709/206, 100, 709/207, 101, 300; 705/41; 707/10

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,632,011	A		5/1997	Landfield et al.
5,765,033	A		6/1998	Miloslavsky
5,826,269	A	*	10/1998	Hussey 707/10
5,961,590	A	*	10/1999	Mendez et al. 709/206
6,282,522	B1	*	8/2001	Davis et al. 235/375
6,381,634	B1	*	4/2002	Tello et al. 709/206
6,405,243	B1	*	6/2002	Nielsen 709/206

OTHER PUBLICATIONS

Scheussler et al., "System and method for identifying users in a distributed network", US patent application Publication US 2002/0107856 A1.*

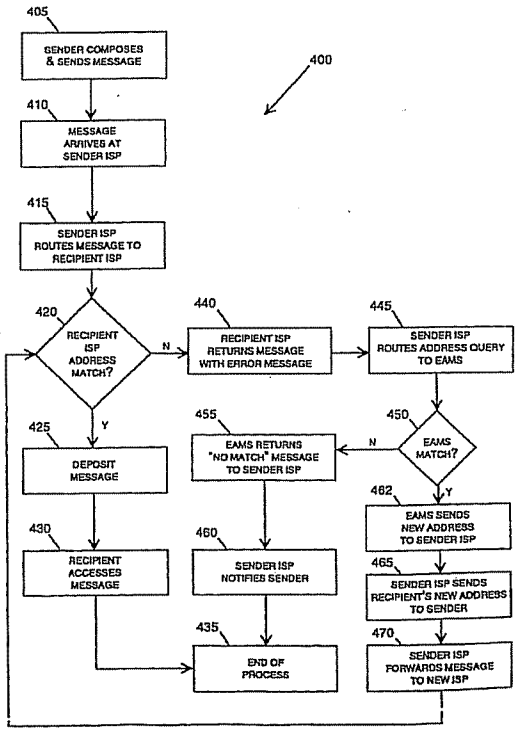
* cited by examiner

Primary Examiner—Majid A. Banankhah
Assistant Examiner—Lilian Vo
(74) *Attorney, Agent, or Firm*—Morris, Manning & Martin, LLP

(57) **ABSTRACT**

A system and methods for managing Internet e-mail address changes, particularly useful for situations where subscribers change Internet service providers. A computer system manages a database of stored records correlating a first e-mail address of an intended recipient, e.g. an old e-mail address, to a second e-mail address, e.g. a new e-mail address of the intended recipient. A program module in the computer system is responsive to an Internet query for accessing the database to determine whether a second e-mail address of the intended recipient is stored in association with a first e-mail address. Another program module is operative for providing the second e-mail address as a response to the query. The query response is communicated to the sender or to the sender's ISP so that an undeliverable message can be resent to the new e-mail address. Also provided are security and authentication measures for ensuring that address change requests are valid and authentic.

46 Claims, 5 Drawing Sheets



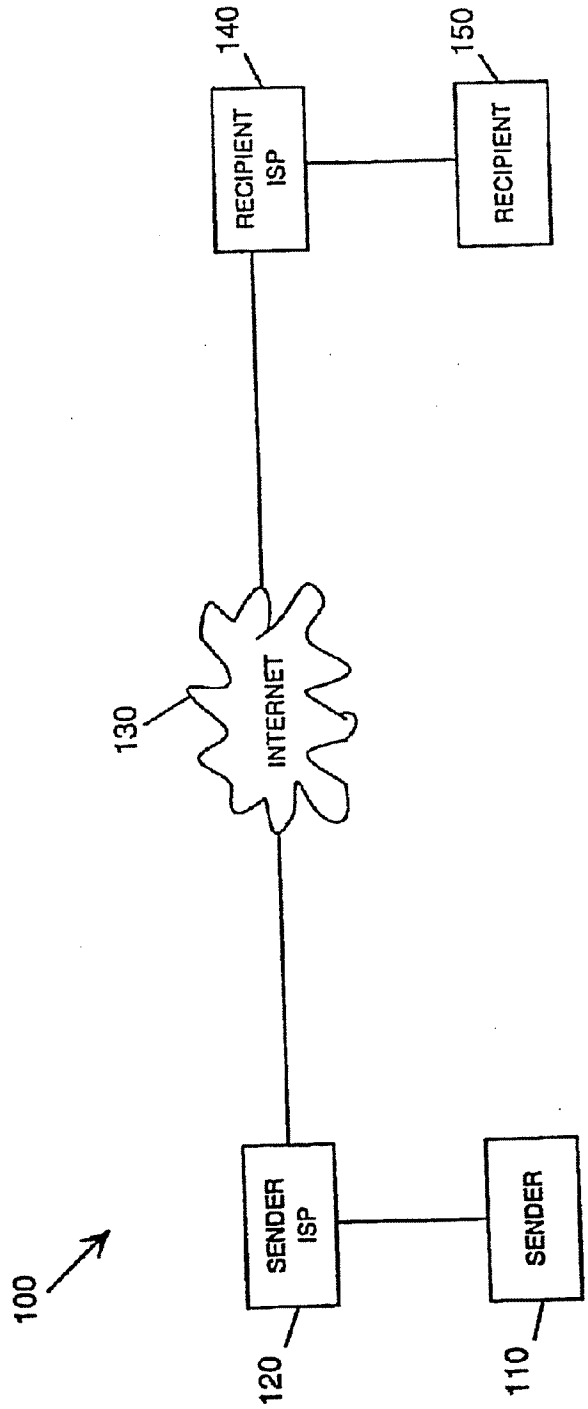
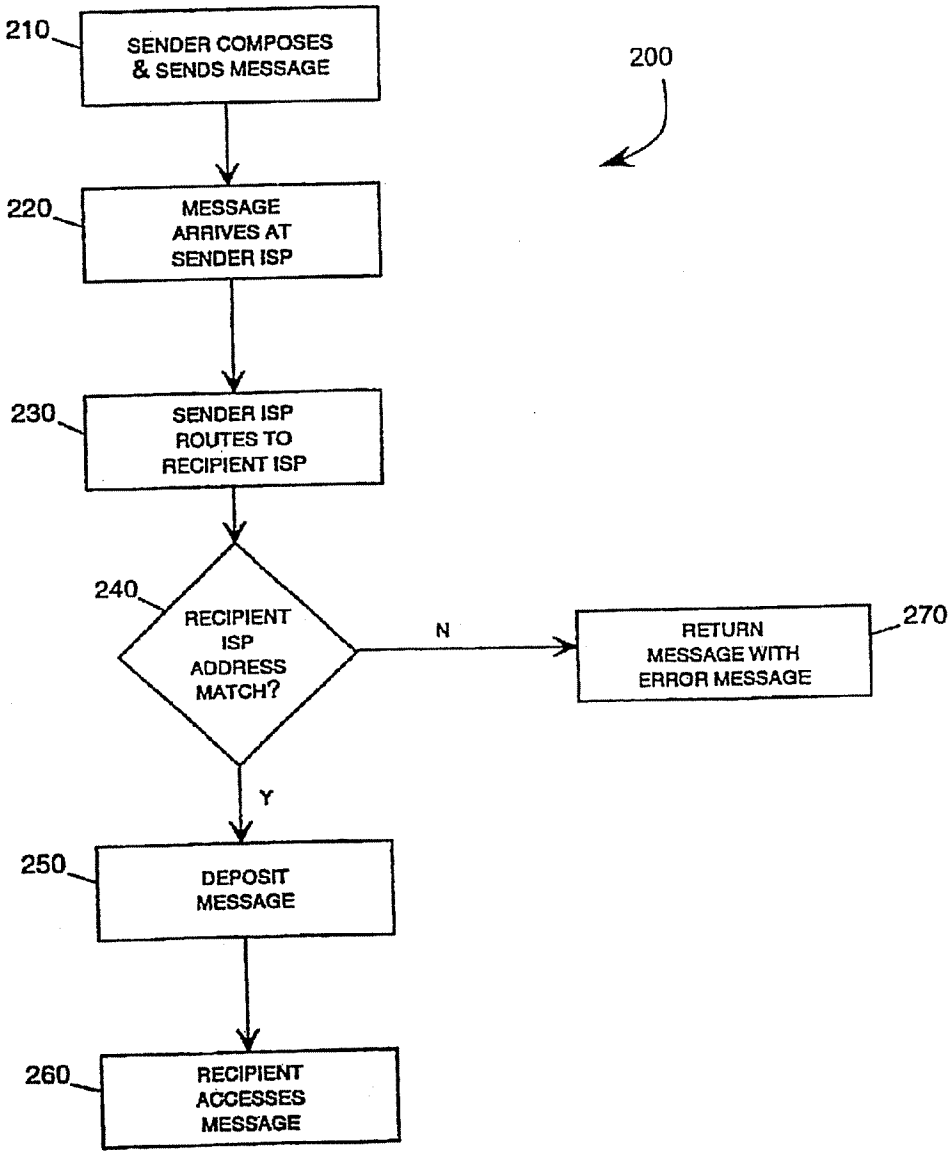


FIG. 1
(PRIOR ART)

FIG. 2
(PRIOR ART)



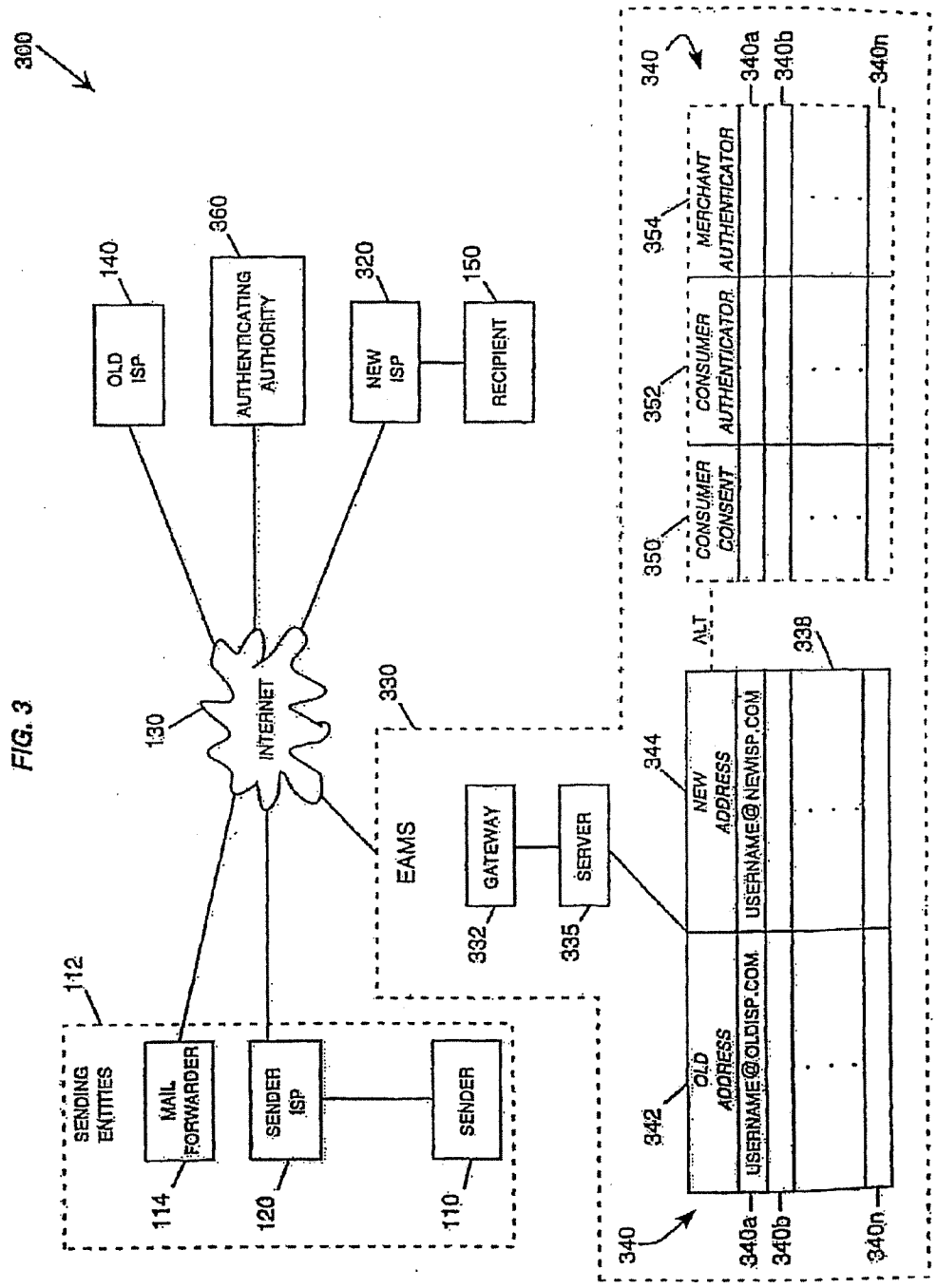

300
140
OLD ISP
360
AUTHENTICATING AUTHORITY
320
NEW ISP
150
RECIPIENT
130
INTERNET
330
EAMS
GATEWAY
332
SERVER
335
112
SENDING ENTITIES
MAIL FORWARDER
114
SENDER ISP
120
SENDER
110
340
340a
340b
340n
ALT
338
342
OLD ADDRESS
USERNAME@OLDISP.COM
344
NEW ADDRESS
USERNAME@NEWISP.COM
350
CONSUMER CONSENT
352
CONSUMER AUTHENTICATOR
354
MERCHANT AUTHENTICATOR

FIG. 3

FIG. 4

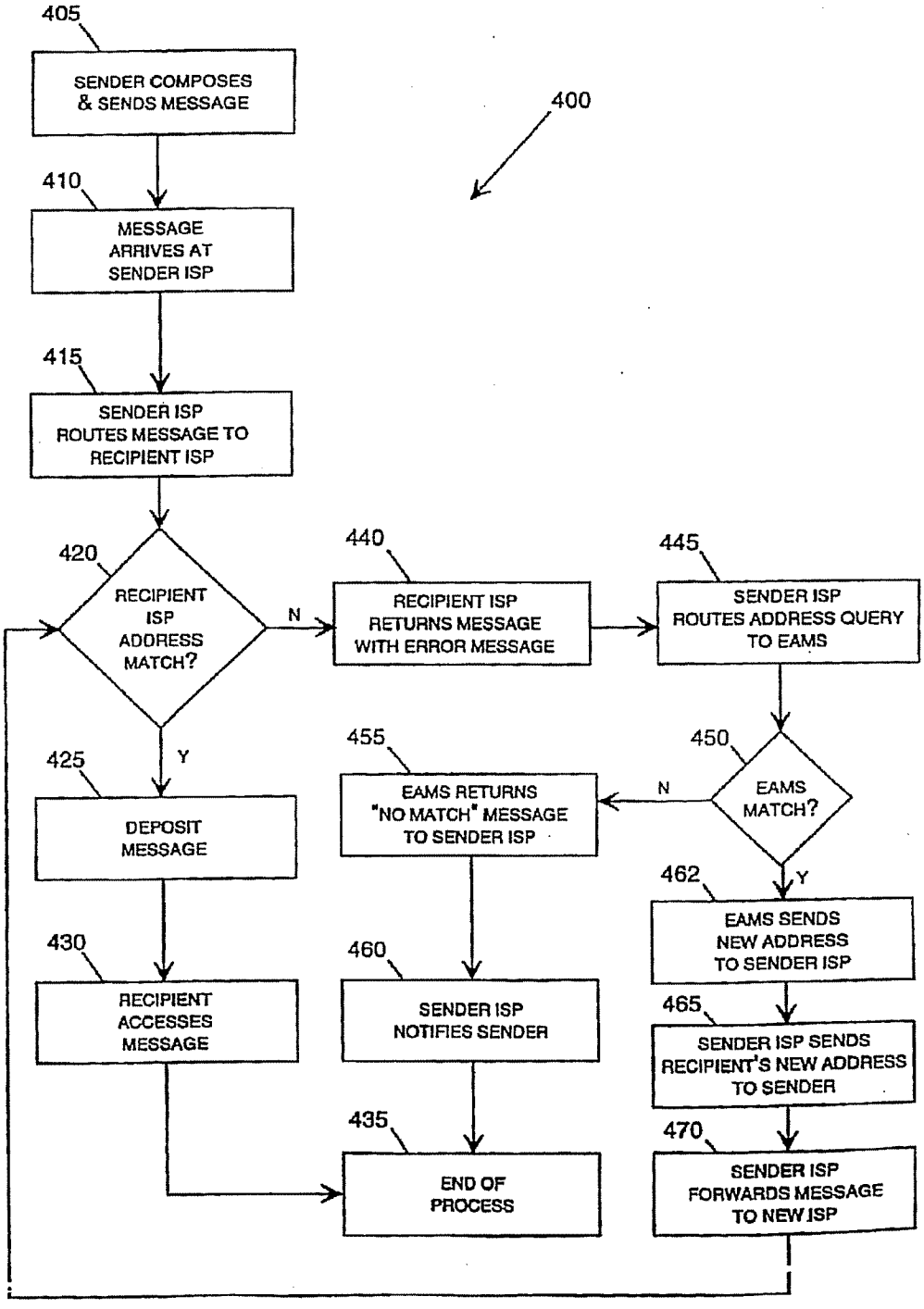
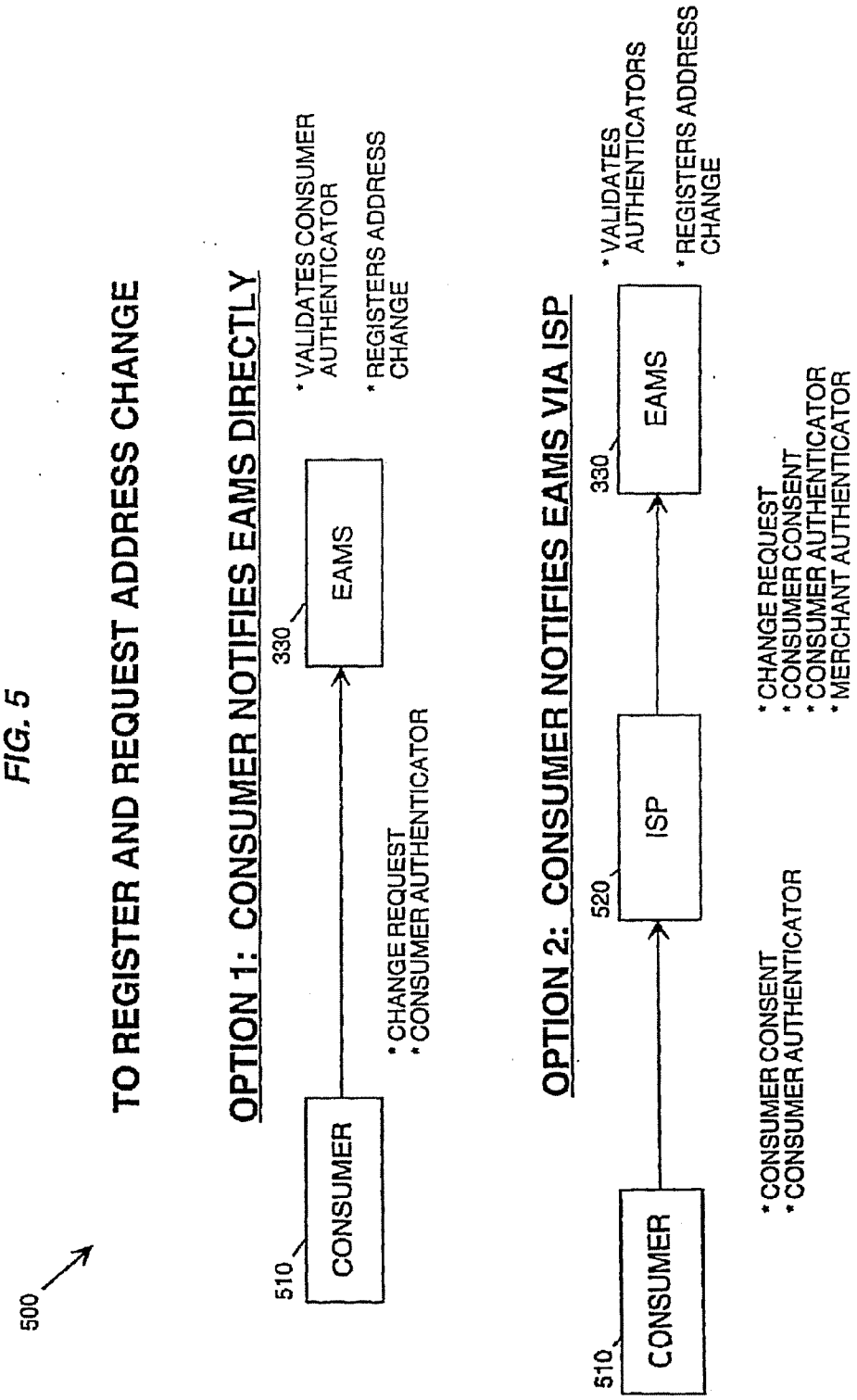

405
SENDER COMPOSES & SENDS MESSAGE
400
410
MESSAGE ARRIVES AT SENDER ISP
415
SENDER ISP ROUTES MESSAGE TO RECIPIENT ISP
420
RECIPIENT ISP ADDRESS MATCH?
N
440
RECIPIENT ISP RETURNS MESSAGE WITH ERROR MESSAGE
445
SENDER ISP ROUTES ADDRESS QUERY TO EAMS
Y
425
DEPOSIT MESSAGE
455
EAMS RETURNS "NO MATCH" MESSAGE TO SENDER ISP
450
EAMS MATCH?
N
Y
462
EAMS SENDS NEW ADDRESS TO SENDER ISP
430
RECIPIENT ACCESSES MESSAGE
460
SENDER ISP NOTIFIES SENDER
465
SENDER ISP SENDS RECIPIENT'S NEW ADDRESS TO SENDER
435
END OF PROCESS
470
SENDER ISP FORWARDS MESSAGE TO NEW ISP

FIG. 5


500
TO REGISTER AND REQUEST ADDRESS CHANGE
OPTION 1: CONSUMER NOTIFIES EAMS DIRECTLY
510
CONSUMER
330
EAMS
*CHANGE REQUEST
*CONSUMER AUTHENTICATOR
*VALIDATES CONSUMER AUTHENTICATOR
*REGISTERS ADDRESS CHANGE
OPTION 2: CONSUMER NOTIFIES EAMS VIA ISP
510
CONSUMER
520
ISP
330
EAMS
*CONSUMER CONSENT
*CONSUMER AUTHENTICATOR
*CHANGE REQUEST
*CONSUMER CONSENT
*CONSUMER AUTHENTICATOR
*MERCHANT AUTHENTICATOR
*VALIDATES AUTHENTICATORS
*REGISTERS ADDRESS CHANGE

SYSTEM AND METHOD FOR ELECTRONIC MAIL (E-MAIL) ADDRESS MANAGEMENT

TECHNICAL FIELD

The present invention relates generally to electronic mail on the Internet (also called e-mail and email), and more particularly relates to a system and methods for managing e-mail addresses to effect the delivery of e-mail messages when a subscriber abandons an e-mail address and obtains a new e-mail address, as when a subscriber changes Internet service providers ("ISPs").

BACKGROUND OF THE INVENTION

The Internet is a collection of computers, networks, routers, and gateways that use the TCP/IP suite of protocols to connect computers all over the world. The Internet links computers together in a way such that they can transfer information to each other. Computer users often subscribe to communication services provided by an Internet Service Provider ("ISP") to access and utilize the Internet.

One of the popular uses of the Internet is to send and receive electronic messages, which are often referred to as electronic mail or "e-mail." E-mail is a computer-to-computer version of interoffice mail or the postal service. E-mail enables computer users to send and receive messages over a computer network. Delivered messages are stored in electronic mailboxes that are assigned to users on the network. Messages received in a mailbox can be viewed, saved, or deleted by a recipient using known and popular electronic mail computer software such as CE Software's QUICKMAIL™, OUTLOOK™ made by Microsoft Corporation, EUDORA™ made by Qualcomm, and the like.

In order to deliver e-mail, an addressing scheme is required. Each computer on the Internet is assigned a numeric Internet protocol ("IP") address, which is a part of the TCP/IP protocol. The IP address in the current TCP/IP scheme consists of four discrete numbers, each less than 256, separated by dots (e.g., 123.4.5.678). A distinct IP address is assigned to each different computer that is connected to the Internet. Because numeric IP addresses are difficult for people to remember, the custom has arisen to utilize domain names for computers on the Internet rather than the IP numbers themselves.

Typical e-mail messages are addressed to a recipient in the form of "username@domain_name.domain," where username is a form of name for a message recipient, domain_name is a lower level domain name assigned to an organization or an ISP, and domain is a top level domain name. Present top level domain names are limited and can be the U.S. government (.gov), the U.S. military (.mil), a network (.net), a commercial enterprise (.com), an educational institution (.edu), or a country (e.g., .jp for Japan or .uk for the United Kingdom). For example, Joe Smith might subscribe to Internet service provided by a commercial enterprise or ISP called "Braincoil, Inc." and be given an e-mail address in the form of joe_smith@braincoil.com.

A computer called a domain name server ("DNS") translates between the domain_name.domain portion of an e-mail address and the numeric Internet protocol ("IP") address. When a message with an e-mail address is received at an ISP from one of its subscribers, the ISP employs a DNS to look up the numeric IP address associated with the e-mail address. Using the IP address of the message, the ISP transmits the message to an electronic device called a router, which selects one of possibly several different data communication paths connected to another computer and sends the message to the other computer. The message is passed from computer to computer, via their respective connected routers, until the message arrives at a computer associated with the ultimate intended recipient. Typically, the final computer to receive the message is a computer operated by the ISP to which the recipient subscribes. The message is then stored in a mailbox associated with the subscriber, and the subscriber is often notified via e-mail software that he or she has mail in the mailbox.

A particular problem encountered in today's usage of the Internet is the movement of subscribers from one organization to another, such as from one ISP to another. There are many reasons for subscribers to change ISPs, including a geographical move from one part of the country to another, a change to obtain a more favorable pricing plan, and a dissatisfaction with the service provided by an ISP. Changing ISPs typically means that a subscriber's e-mail address will change, unbeknownst to people who wish to send that subscriber a message. For example, Braincoil subscriber Joe Smith might have originally had an address such as joe_smith@braincoil.com. If Joe Smith moves his Internet service to a new and different ISP called "Headspiral", he might acquire a new e-mail address such as joe.smith@headspiral.com. Although it might be desirable to have a person keep his e-mail address on a permanent basis, the present scheme of addressing typically mandates that changing ISPs results in changing e-mail addresses.

People who wish to send Joe Smith a message may not know that Joe Smith has changed ISPs and thus has a new e-mail address. After a person changes ISPs, his old e-mail address at his old, former ISP becomes invalid. Messages sent to an invalid e-mail address typically "bounce" back from the intended recipient's old ISP to the sender's ISP. Stated in other words, the old ISP cannot deliver the message to the recipient, who is no longer a subscriber. In this case, the old ISP typically sends a predetermined message back to the sender's ISP that the message is undeliverable. This predetermined "bounce" message often includes a text string containing the text "message undeliverable". The predetermined bounce message is delivered to the sender to inform him or her that there is a problem with delivery of the message.

After a sender receives a bounce message, the sender may conduct a search on the Internet or may attempt to contact the intended recipient by other means (e.g., telephone) in order to obtain the intended recipient's new e-mail address. If the sender succeeds in finding the new e-mail address, he can send the message again, though a delay in delivery of the message has resulted. On the other hand, if the sender cannot find the new e-mail address, then the message cannot be delivered at all.

It would be helpful if ISPs maintained a list correlating old e-mail addresses and new e-mail addresses and updated the list when subscribers terminated their subscriptions. That way, they could provide a forwarding service. However, ISPs typically have no financial incentive to forward messages intended for former subscribers. Message forwarding requires use of computer and bandwidth resources for which ISPs will typically receive no payment. Thus, a need exists for a system and methods that facilitate delivery of e-mail when a person obtains a new e-mail address and his or her old e-mail address becomes invalid.

SUMMARY OF THE INVENTION

Briefly described, the present invention comprises a system and methods for managing e-mail address changes. The

preferred system comprises a computer for managing a database of stored records correlating a first e-mail address of an intended recipient to a second e-mail address of the intended recipient. A program module in the computer system is responsive to an Internet query from a sender of an e-mail message based on the first e-mail address of the intended recipient. The program module accesses the database to determine whether a second e-mail address of the intended recipient is stored in association with the first e-mail address. Another program module in the computer system, which is responsive to a determination that a second e-mail address of the intended recipient is stored in association with the first e-mail address, retrieves the second e-mail address as a response to the query. Furthermore, a program module is provided for communicating the query response to the sender.

A principal use of the invention will be in situations wherein the first e-mail address is an invalid old address associated with a former Internet service provider (ISP) of the intended recipient, and the second e-mail address is a new e-mail address associated with a new ISP of the intended recipient.

Preferably, the computer systems utilized in implementing the present invention are Internet accessible, and the query and query response are communicated via Internet messaging protocols.

According to another aspect of the invention, a computer system automatically forwards the e-mail message to the second e-mail address in response to receipt of the query response. In one embodiment, it is a computer system associated with the sender of the e-mail message that automatically forwards the e-mail message to the second e-mail address in response to receipt of the query response. More specifically, the query response is provided to an ISP associated with the sender, and the sender's ISP autoforwards the e-mail message to the second e-mail address. Alternatively, the query response may be provided directly to the sender, and the sender's computer is operative to readdress and resend the e-mail message.

According to yet another aspect of the invention, there is provided a program module for creating a new record in the database in response to receipt of an address change request from a consumer. For security purposes, such as ensuring that address changes requests are authentic, the program module for creating a new record in the database is operative for requiring predetermined authenticating information before creating a record in the database. This authenticating information is preferably obtained from an Internet accessible authenticating authority. Various types of authenticating information may be required, such as a consumer authenticator identifying the person that requested the address change or a merchant authenticator identifying the ISP from which the address change request originated.

In embodiments of the invention that include the security features, the database stores other predetermined information in association with the first e-mail address and the second e-mail address, such other information selected from the group comprising a consumer consent, consumer authentication, and merchant authentication.

In addition to implementing the present invention with systems operative as described above, the present invention may also be embodied as computer-implemented methods for carrying out the various e-mail address management and address change operations of the invention.

Accordingly, it is an object of the present invention to provide a system and methods for managing e-mail addresses for situations where subscribers change ISPs and obtain a new e-mail address.

It is another object of the present invention to provide a system for e-mail address management that facilitates delivery of e-mail for new subscribers of an ISP by providing an address matching service between old e-mail addresses of subscribers and their new e-mail addresses.

These and other objects, features, and advantages of the present invention will become more clear upon reference to the accompanying drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating the present known system for communicating e-mail messages from a sender to an intended recipient via the Internet.

FIG. **2** is a flow chart illustrating the known process by which present day e-mail systems handle e-mail delivery and error messages in the event of failed delivery.

FIG. **3** is a block diagram illustrating an Internet-based system for communicating e-mail messages from a sender to an intended recipient constructed in accordance with the present invention.

FIG. **4** is a flow chart illustrating the process carried out by the preferred system of FIG. **3**.

FIG. **5** illustrates the process by which a person registers an address change and authentication steps for use in the preferred system of FIG. **3**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to the drawings, in which like numerals indicate like elements and/or components throughout the several figures, FIG. **1** illustrates the present general Internet environment **100** in which electronic mail operates. A sender **110** is a person who wants to send an e-mail message to an intended recipient **150**. The sender **110** subscribes to Internet service via a sender Internet service provider (ISP) **120**. The sender **110** believes the intended recipient **150** is another computer user who subscribes to a recipient ISP **140**. The sender ISP **120** and the recipient ISP **140** are connected for data communications through a data network such as the Internet **130**, which is represented as a "cloud" to indicate its amorphous, widely distributed nature.

FIG. **2** illustrates the known prior art process **200** that is followed when an e-mail message is sent from a first user at one ISP (the sender **110**) to an intended recipient. Starting at step **210**, the sender **110** composes an e-mail message. He then addresses that e-mail with an address he believes to be the correct one for the intended recipient. As described above, an e-mail address is formatted to comprise two pieces of information: 1) recipient's username (which corresponds to the mailbox the sender believes the intended recipient has at an ISP), and 2) the domain name and domain associated with the recipient ISP **140**. After composing and addressing the message, the sender **110** then sends the message from his computer utilizing known e-mail computer software.

After the sender **110** sends the message, step **220** is performed. In step **220**, the message arrives at the sender ISP **120**. Next, in step **230**, the sender ISP **120** routes the message to the recipient ISP **140** using the address that was provided with the message. The sender ISP **120** typically does this by employing a domain name server (DNS) to translate the address provided with the message into a numeric IP address. Using the IP address, the sender ISP **120**

sends the message over the Internet through the proper mail gateway (not shown). After traveling over the Internet **130**, the message arrives at the recipient ISP **140**.

Next at step **240**, the recipient ISP **140** determines whether there is an address match. That is, the recipient ISP **140** determines if the mailbox specified in the username portion of the e-mail address exists at that ISP. This step is effected by reference to a stored list of valid addresses associated with the recipient ISP.

If there is an address match, the recipient ISP **140** deposits the message in the mail box of the recipient **150** at step **250**. Once a message has been deposited in the recipient's mailbox, the recipient can access that message in step **260** through a computer connected to the recipient ISP **140**.

If, at step **240**, there is no address match for the e-mail message at the recipient ISP **140**, then step **270** is performed. At step **270**, the recipient ISP **140** returns the message to the sender in the known manner along with an error message (also called a "bounce" message) because the intended recipient does not have the mailbox specified in the address at the recipient ISP. The recipient ISP **140** returns the message by sending it back over the Internet **130** to the sender ISP **120**. In turn, the sender ISP transmits the error message to the mailbox of the sender **110**. As previously described, a typical error message contains the text string "message undeliverable." Although most present day e-mail systems typically include this "message undeliverable" text string, those skilled in the art will appreciate that other mechanisms or text strings can exist or be created to indicate the fact that an e-mail message cannot be delivered to a particular mailbox, and that such other mechanisms or text strings may serve as an indication that a "message" is "undeliverable" within the scope of the present invention.

Now that the known e-mail process **200** has been described, one can better appreciate what events may lead a message to be returned to a sender because the message could not be delivered to the intended recipient. In particular, one common situation merits special mention.

Suppose the intended recipient was at one time connected to the Internet through an ISP called Old ISP. While the recipient had a mailbox at Old ISP, he distributed his e-mail address to many others, including sender. At a later time, suppose that the intended recipient changed ISPs from Old ISP to a different ISP called New ISP. In doing so, the intended recipient's mailbox at Old ISP was removed, and he got a new mailbox at New ISP. Along with the mailbox change, of course, came an address change from an old e-mail address to a new address. However, the intended recipient's old address was so widely distributed that he may have been unable to inform every friend and acquaintance of his new address. Further suppose that the sender was one of those people that the intended recipient failed to inform of the new address.

Now, suppose that the sender wants to send a message to the intended recipient. Not having been informed otherwise, the sender assumes that the intended recipient can still receive e-mail at the old address. When the sender sends a message to the intended recipient at the old address, it is returned to him with an error message because Old ISP is unable to find an address match.

If, at that point, the sender still wants the intended recipient to receive the message, he will first have to conduct a search to find the intended recipient's new address. If the sender succeeds in finding the intended recipient's new e-mail address, he must then once again send the message, this time to the new address.

Clearly, the described problem inconveniences both senders and intended recipients. It also poses a burden to any ISP attempting to win over customers from other ISPs. Many people have a natural resistance to change; once an e-mail address has been widely disseminated, there is a disincentive to obtain a new address because of the inconvenience of notifying a large number of people of the new address. Therefore, there is a need in the art to reduce the inconveniences caused by users changing ISPs and/or addresses.

The present invention makes the process of sending e-mail function more smoothly through a system and methods for managing e-mail addresses, especially e-mail addresses that have changed. In this manner, the present invention allows reduction of the inconveniences caused by a user changing his or her ISP or address.

Referring next to FIG. **3**, a general Internet architecture **300** that includes an E-mail Address Management System ("EAMS") **330** constructed in accordance with the preferred embodiment of the present invention is shown and will be described. The preferred EAMS **330** is a computer-implemented database system comprising a gateway **332**, a computer server **335**, and a memory or database **338** constructed as a database look-up table that correlates an old e-mail address to a new e-mail address for each participant. For example, the recipient **150** at one time was a user of Old ISP **140** and had an old mailbox at Old ISP with an old address. At a later time, the recipient **150** changed ISPs to New ISP **320** and obtained a new mailbox at New ISP with a new address.

In the preferred system, the recipient **150** registers his or her address change with the EAMS **330** in order to have information about the address change in the database **338**. The registration process is discussed in more detail later. As described above, the preferred EAMS **330** contains an old address and a new address for each address change registered with the EAMS **330** and stored in the database **338**. Preferably, this address change information is stored in the form of a data record **340** having a plurality of data fields, including an old e-mail address field **342** and a new e-mail address field **344**. The fields of a plurality of these records may be indexed for searching or otherwise stored so that they can be retrieved in accordance with known database techniques.

The EAMS **330** is connected to the Internet **130** and thus is accessible by any ISP that is connected to the Internet and can send and receive e-mail messages. Other types of communications between the EAMS **330** and ISPs are possible and contemplated in the present invention, such as file transfer protocol (ftp) messaging, hypertext transfer protocol (http) messaging, and customized messaging using the TCP/IP protocol. However, the known Internet e-mail messaging protocol is preferred for its simplicity and wide acceptability.

Also shown in FIG. **3** is an authenticating authority **360** connected to the Internet **130**. The authenticating authority **360** is one of several known types of systems. that provide computer-based authentications, such as a certificate authority. One example of a known authenticating authority is the Cybertrust, operated by GTE. An authenticating authority **360** may be involved in the present invention in embodiments wherein the EAMS **330** , for security and fraud prevention purposes, requires certain authenticating information from subscribers before accepting data that correlates a new e-mail address to an old e-mail address.

According to another aspect of the invention, described in more detail below, the database **338** also stores predeter-

mined information associated with an old e-mail address and new e-mail address. By way of example but not limitation, this information may include consumer consent information, consumer authenticator information, and merchant authenticator information and may be stored in separate but associated fields **350**, **352**, and **354**, respectively, of the record **340**. Such additional fields are preferably provided for purposes of security, troubleshooting, and dispute handling.

Generally, the EAMS **330** is operative to receive from any source queries in the form of predetermined messages containing an e-mail address. In response to receiving a query, the EAMS **330** can look up the e-mail address in the database **338** in order to determine if the e-mail address is associated with a new e-mail address. In one embodiment of the present invention, the query to the EAMS **330** may include a message that the EAMS **330** automatically forwards ("autoforwards") to the new address if a new address is found.

Alternatively, the EAMS **330** is not operative to automatically forward a message even if a new address is found after searching the database **338**. Instead, if the database **338** correlates a new address with the address sent in the query, the EAMS **330** informs the entity which sent the query about the new address. On the other hand, if the database **338** does not have a new e-mail address associated with the address sent in the query, the EAMS **330** informs the entity which sent the query of this fact. Various embodiments of the present invention are possible in which different entities query the EAMS **330**. A few of these exemplary embodiments are now discussed in more detail.

In the preferred embodiment of the present invention, the sender ISP **120** is configured to autoforward e-mail containing an old address to a new address. If a message is sent to an intended recipient at the old address, the message is returned to the sender ISP **120** with an error message, since there is no address match at Old ISP **140**. At that point, the sender ISP **120** queries the EAMS **330** over the Internet **130** to find out if there is an address change registered with the EAMS for the old address. Then, the EAMS **330** searches its database to see if it contains a record relating the old address to a new address. If a new address is found for the old address, then the EAMS **330** sends the new address back to the sender ISP **120**. With the new address, the sender ISP **120** automatically forwards the message to the intended recipient **150** at the new ISP **320** and notifies the sender **110** via e-mail of the intended recipient's new address. If the EAMS **330** does not find a record relating an old address to a new address, then the EAMS **330** preferably notifies the sender ISP **120** of this fact. In this case, the sender ISP **120** then notifies the sender **110** via e-mail that the message could not be delivered to old address and that there was no forwarding address registered with the EAMS **330**.

In another embodiment of the invention, a sender **110** who Dreceives a bounce message can himself or herself query the EAMS **330** over the Internet **130** to determine if the intended recipient **150** has registered an address change with the EAMS **330**. In such an embodiment, the query may be conducted via e-mail. Alternatively, the EAMS **330** may have a web site interface (i.e., an http interface) that allows a sender **110** to input an e-mail address and determine if that e-mail address is correlated with a new e-mail address. This aspect of the invention is useful where the ISP of the sender **110** is not configured to automatically query the EAMS **330** to obtain a new e-mail address in response to receipt of a bounce message. In this situation, the sender **110** who finds a new address after making a query of the EAMS **330** can then use the new address to resend the message that caused the bounce message in the first place. The sender **110** may also want to query the EAMS **330** about an address change if the sender suspects, even before sending an e-mail, that the intended recipient **150** has changed addresses.

In yet another embodiment of the present invention, a sender may be provided with forwarding software that is stored on the sender's computer. The forwarding software is responsive to receipt of a bounce message indicating that a message previously sent by the sender could not be delivered (i.e., the software is automatically responsive to the text string "message undeliverable" contained in an e-mail message). Upon receiving such a bounce message, the forwarding software can initiate a query to the EAMS **330** to determine if the EAMS **330** has a record associating a new e-mail address with the e-mail address of the message that could not be delivered. The EAMS **330** then notifies the forwarding software preferably via e-mail, of the results of the query, and the EAMS **330** includes the new address if one is found. Upon notification that there exists a new address, the forwarding software automatically forwards the message that previously could not be delivered to the new address.

In FIG. **3**, a mail forwarder **114** is also shown connected to the Internet **130**. A mail forwarder **114** is capable of receiving an e-mail message at a given e-mail address over the Internet. After receiving the e-mail message, the mail forwarder **114** then sends the message back out onto the Internet to another Internet address. The address to which the e-mail message is forwarded may be determined by software used to operate the mail forwarder **114**, or alternatively the mail forwarder may look to the contents of the e-mail itself for instructions on where to send the e-mail.

The mail forwarder **114**, the sender ISP **120**, and the sender **110** are all sending entities **112** that are capable of sending and receiving e-mail messages. One skilled in the art should recognize that various embodiments of the present invention are possible in which any one of the sending entities attempts to send an e-mail message using a first address, receives a "message undeliverable" error, queries the EAMS **330** based on the first address, receives a second address over the Internet from the EAMS **330** in response to the query, and then resends the e-mail message using the second address.

FIG. **4** is a flowchart illustrating a computer-implemented process or method **400** for sending an e-mail in accordance with the preferred embodiment of the present invention. The described process assumes that a sender ISP is configured to access an EAMS **330** over the Internet in the event that a message is returned to it which is undeliverable.

The method **400** is preferably implemented as one or more computer application programs, operative to run on a computer apparatus comprising a central processing unit, main memory, permanent read/write memory (hard disk, floppy disk, etc.), display, keyboard, and mouse. Such elements of a computer apparatus are known to those skilled in the art and will not be described further herein. It will further be appreciated that the steps of FIG. **4** are carried out in several different computer devices connected, for example, via the Internet. These computer devices comprise a computer system associated with the message sender, a computer system associated with the message sender's ISP, a computer system associated with the intended recipient's old ISP, a computer system associated with the intended recipient's new ISP, and a computer system associated with an EAMS **330** constructed and operative as described herein. The discussion which follows will enable one skilled

to the art to understand which portions or parts of the process **400** are applicable to and carried out in which computer system.

Starting in FIG. **4** at step **405**, a sender composes a message at his or her computer and addresses it to the address believed to be correct for an intended recipient. The sender then sends the message from his computer to a computer system that provides Internet access, which is typically the ISP at which the sender maintains an Internet service subscription. An example of the ISP to which the sender may send his message is the sender ISP **120** of FIG. **3**. It will, however, be appreciated that a message need not be sent to a specific ISP at which the sender maintains a subscription; rather, in accordance with the invention, the message may be sent to any computer system that provides Internet access, which for purposes of this description serves as the "sender ISP".

At step **410**, the message arrives at the sender ISP. At step **415**, the sender ISP chooses a particular mail gateway in accordance with the IP address of the message and routes the message to the ISP indicated in the message address as the recipient ISP. The message is then sent over the Internet and arrives at the recipient ISP, which is the old ISP **140** in FIG. **3**.

At step **420**, the recipient ISP determines whether there is an address match, i.e., whether the mailbox specified in the address of the received message presently exists at recipient ISP. This is carried out in the known manner by reference to an address table stored at the recipient ISP that correlates subscribers of that ISP and their associated e-mail addresses.

If the recipient ISP finds an address match at step **420**, then step **425** is performed. At step **425**, the recipient ISP deposits the message in the mailbox specified in the address. At step **430**, the intended recipient accesses the message from his mailbox using a computer connected to the recipient ISP. After the intended recipient accesses the message in his mailbox, the process ends at step **435**.

It will be appreciated that the situation of the foregoing steps is identical to that of FIG. **1** and the accompanying text where the intended recipient has a mailbox at the address to which the sender **110** sends the message. If this is the case, it will of course be appreciated that the EAMS **330** does not enter into play. On the other hand, if, at step **420**, there is no match between the e-mail address of the message received at the recipient ISP and the list of valid addresses at the recipient ISP, the "no" branch is followed to step **440** and the method of the present invention comes into play.

At step **440**, the recipient ISP returns the message to the sender ISP over the Internet with an error or bounce message, as previously described. Control then passes to step **445**.

At step **445**, the sender ISP receives the error message and sends an address query to the EAMS **330** over the Internet to determine if there is an address change registered with the EAMS **330** for the address indicated in the returned message. The address query comprises the address for which a new address is sought.

After the EAMS **330** receives the address query, step **450** is performed. In step **450**, the EAMS **330** searches its database, i.e. database **338** FIG. **3**, to see if it contains a record relating a new address to the address contained in the address query. If a new address is found for the address of the address query, then there is an EAMS match.

If there is no EAMS match, control passes to step **455**. There are several reasons for no EAMS match. For example, the reason could be because the intended recipient never had the mailbox specified in the address at the recipient ISP specified in the address. Or, there might be no EAMS match because the intended recipient changed addresses but failed to register the address change with the EAMS **330**. In step **455**, the EAMS **330** notifies the sender ISP that there was no EAMS match.

At step **460**, the sender ISP notifies the sender, typically via e-mail, that the message could not be delivered to the address provided for the message and that there was no address change registered with the EAMS **330** for that address. After step **460**, the process ends at step **435**.

It will of course be appreciated that there will be an EAMS match found at step **450** in the event that the intended recipient has registered his or her address change with the EAMS **330**. A match will also be found at step **450** in the event that the EAMS **330** for some other reason contains a record matching the old e-mail address to a new e-mail address. For example, the present invention contemplates the situation where ISPs transmit address changes to the EAMS **330**. The present invention also contemplates the situation where some other third party provides the EAMS **330** with a list correlating particular e-mail addresses to other e-mail addresses.

Returning to step **450**, if there is an EAMS match for the address provided in the address query from the sender ISP, then control passes to step **462**, in which the EAMS **330** sends the new address over the Internet back to the sender ISP. Once the sender ISP receives the new address, the sender ISP notifies the sender via e-mail of the intended recipient's new address in step **465**.

In step **470**, the sender ISP forwards the message to the intended recipient's new ISP using the new address. After the new ISP receives the message, control passes to step **420**, with the new ISP now serving as the recipient ISP. The message is then delivered to the intended recipient in accordance with the steps subsequent to **420**.

FIG. **5** illustrates a registration process **500** in which persons with e-mail addresses or mailboxes ("consumers") provide information to the disclosed EAMS **330** for the purpose of maintaining the cross reference table or database **338** of FIG. **3**. Typically, the present invention contemplates creation of a new record in the database in response to receipt of an address change request from a consumer. It will be appreciated that there are several ways in which a consumer may provide the requisite information of an e-mail address change to the EAMS **330**.

One way to register an address change is for a consumer **510** to register an address change with the EAMS **330** directly in the form of an address change request. In this case, the consumer **510** provides the EAMS **330** with an address change request comprising predetermined information indicating the identity of the consumer and the e-mail address change. For security purposes and for ensuring that an address change is valid, the EAMS **330** may require certain additional information from the consumer before creating a record correlating the given new e-mail address to an old address. This additional information may include the consumer's social security number, mother's maiden name, employer's ID number, and similar information.

In such an embodiment, however, it will be appreciated that security is not as great as may be desired, and greater assurance of the validity of an address change may be preferred. Therefore, preferred embodiments of the invention will employ devices or methods for increasing assurance of a valid change. Those skilled in the art will understand and appreciate that there are presently several known

methods for authenticating a person's identity and authority in the Internet environment. For example, an authenticating authority, such as the authenticating authority **360** in FIG. **3**, is preferably employed to provide such greater assurance of a valid address change.

In accordance with the preferred embodiments of the invention, the EAMS **330** requires predetermined authentication information prior to effecting an address change. This is to minirize the possibility that an unauthorized person can successfully divert e-mail from a known e-mail address to another address for unlawful purposes such as e-mail interception or as a malicious prank. Preferably, therefore, any registration with the EAMS **330** will include (1) an address change request and (2) a consumer authenticator. The address change request typically includes the consumer **510**'s old e-mail address and new e-mail address, as well as other optional information.

The consumer authenticator simply ensures that the consumer **510** is who he says he is. The consumer **510** can obtain a consumer authenticator by registering with any one of a number of known authentication authorities, such as the authentication authority **360** in FIG. **3**, that are approved by the entity running the EAMS **330**. The address change registration and the registration with the authentication authority may, but need not, be transacted electronically over the Internet **130**.

Once the EAMS **330** receives the address change request and consumer authenticator, it first validates the consumer authenticator. This is typically effected by contacting the authenticating authority in the known manner. After validation, the EAMS **330** creates a record in its database **338** so that it can provide the new address in response to an address query on the old address.

Alternatively, and still referring to FIG. **5**, there is a second way to register an address change. In this second option, the consumer **510** who has obtained a new e-mail address with an ISP **520** first provides the ISP **520** with predetermined information comprising (1) a consumer consent and (2) a consumer authenticator. The consumer consent ensures that the consumer **510** wants his or her address change registered with the EAMS **330** . The consumer authenticator is the same as that used in the first registration option and can be obtained as already explained.

Once the ISP **520** has both the consumer consent and the consumer authenticator, the ISP preferably submits certain predetermined information, typically via e-mail or other Internet communication, to the EAMS **330** . This predetermined information preferably comprises (1) a change request, (2) the consumer consent, (3) the consumer authenticator, and (4) a merchant authenticator. Although all of this information is not required in all embodiments, certain combinations of this information are preferred for use in the present invention to provide for adequate assurances of security and privacy for the ISP's customers.

Typically, the change request will include as minimum required information the old e-mail address and the new e-mail address of the consumer **510**. Furthermore, it is also contemplated that the ISP **520** may retain the consumer authenticator and provide the merchant authenticator in embodiments where the EAMS **330** only requires provision of the merchant authenticator. This configuration may be more attractive in certain situations, such as when the ISP **520** is configured to store consumer consents and authenticators and the EAMS **330** is configured to store merchant authenticators.

The merchant authenticator comprises predetermined information that ensures that the ISP **520** is a legitimate ISP and is reauthorized and/or recognized by the EAMS **330** as an entity from whom the EAMS **330** accepts address changes. In accordance with an aspect of the invention, the EAMS **330** can refuse to accept address change requests from ISPs that are known to be "outlaw" or have developed a history of customer problems or unauthorized address changes. As in the case of consumer authentication, ISPs can obtain a merchant authenticator by registering with any one of a number known authentication authorities approved and/or recognized by the entity running the EAMS **330**. All registrations may, but need not, be transacted electronically over the Internet **130**.

Once the EAMS **330** receives the required predetermined information, e.g. change request, consumer consent, consumer authenticator, and merchant authenticator, it first validates both the consumer authenticator and the merchant authenticator. This is carried out in the known manner by reference to the applicable authorities that issued the authenticators. After validation, the EAMS **330** creates a record in its database **338** containing the old e-mail address in association with the new e-mail address so that it can provide the new address in response to an address query on the old address. In addition, according to another aspect of the invention, information corresponding to the change request, consumer consent, consumer authenticator, and merchant authenticator are stored in the database **338** so that such information can be retrieved and referenced in the event of a later difficulty or dispute.

Now that the address change registration process has been explained, another embodiment of the present invention is discussed. Those skilled in the art will recognize that when an old ISP **140** receives a message that it cannot deliver because there is no address match, it is possible for the old ISP to send an address query on the address to the EAMS **330** instead of immediately sending the message back to the sender ISP **120** with an error message and letting the sender ISP conduct the address query. Once the old ISP **140** receives the results of the address query, the old ISP can act on the results just as the sender ISP **120** would have acted had the sender ISP conducted the address query. It will therefore be appreciated that the present invention is not limited to a situation in which the sender's ISP queries the EAMS **330** with the old address. Rather, the invention is operative in any situation where an Internet entity becomes aware of the inability to deliver an e-mail message due to such circumstances as an address being invalid, outdated, or changed.

Other alternative embodiments of the present invention will become apparent to those skilled in the art without departing from its spirit and scope. The preferred embodiment of the present invention has been disclosed by way of example and it will be understood that other modifications may occur to those skilled in the art without departing from the scope and the spirit of the appended claims.

What is claimed is:

1. A method for effecting delivery of an e-mail message from a sender to an intended recipient, the sender having an Internet service provider (ISP) operative to transmit e-mail messages, the intended recipient associated with an undeliverable first e-mail address associated with a first Internet service provider (ISP) and currently associated with a second e-mail address associated with a second Internet service provider (ISP), comprising the computer implemented steps of:

providing a database of stored records correlating the first e-mail address of the intended recipient to the second e-mail address of the intended recipient;

in response to receipt at the sender's ISP of a "message undeliverable" message from the first ISP in response to the e-mail message being undeliverable to the first e-mail address, communicating a query from the sender's ISP to the database, the query including the undeliverable first e-mail address;

receiving at the database the query from the sender's ISP;

in response to the query, accessing the database to determine whether the second e-mail address of the intended recipient is correlated with the first e-mail address;

in response to a determination that the second e-mail address of the intended recipient is correlated with the first e-mail address, retrieving the second e-mail address as a response to the query and generating a query response including the second e-mail address;

communicating the query response to the sender's ISP;

at the sender's ISP, utilizing the second e-mail address received in the query response as the address for the e-mail message; and

automatically transmitting the e-mail message from the sender's ISP to the second ISP associated with the second e-mail address without the sender's involvement.

2. The method of claim **1**, wherein the first e-mail address is an invalid old address associated with a former Internet service provider (ISP) of the intended recipient and the second e-mail address is a new e-mail address associated with a new ISP of the intended recipient.

3. The method of claim **1**, wherein the database is stored in an Internet accessible electronic mail address management system (EAMS), and the query and query response are communicated via Internet messaging protocols.

4. The method of claim **1**, wherein a computer system associated with the database automatically forwards the e-mail message to the second e-mail address in response to the query response.

5. The method of claim **1**, further comprising steps for creating a new record in the database in response to receipt of an address change request from a consumer having an e-mail box.

6. The method of claim **5**, further comprising the step of requiring predetermined authenticating information before creating the new record in the database.

7. The method of claim **6**, wherein the authenticating information is obtained from an Internet accessible authenticating authority.

8. The method of claim **6**, wherein the authenticating information comprises a consumer authenticator.

9. The method of claim **6**, wherein the authenticating information comprises a merchant authenticator.

10. The method of claim **1**, wherein the database stores other predetermined information in association with the first e-mail address and the second e-mail address, such other information selected from the group comprising a consumer consent, consumer authentication, and merchant authentication.

11. A system for managing e-mail address changes, comprising:

a computer system;

a database of stored records in the computer system correlating a first e-mail address of an intended recipient to a second e-mail address of the intended recipient;

a program module in the computer system responsive to a query from a sender's Internet service provider (ISP) associated with a sender of an e-mail message based on the first e-mail address of the intended recipient for accessing the database to determine whether the second e-mail address of the intended recipient is stored in association with the first e-mail address;

a program module in the computer system, responsive to a determination that the second e-mail address of the intended recipient is stored in association with the first e-mail address, for retrieving the second e-mail address as a response to the query; and

a program module in the computer system for communicating the query response to a process for utilization in automatically re-transmitting the e-mail message to the second e-mail address without the sender's involvement.

12. The system of claim **11**, wherein the first e-mail address is an invalid old address associated with a former Internet service provider (ISP) of the intended recipient and the second e-mail address is a new e-mail address associated with a new ISP of the intended recipient.

13. The system of claim **12**, wherein the Internet query is generated by an Internet service provider (ISP) associated with the sender in response to receipt of a "message undeliverable" message received from the former ISP when the e-mail message was sent to the first e-mail address.

14. The system of claim **11**, wherein the computer system is Internet accessible, and the query and query response are communicated via Internet messaging protocols.

15. The system of claim **11**, further comprising a program module for creating a new record in the database in response to receipt of an address change request from a consumer.

16. The system of claim **15**, wherein the program module for creating a new record in the database is operative for requiring predetermined authenticating information before creating a record in the database.

17. The system of claim **16**, wherein the authenticating information is obtained from an Internet accessible authenticating authority.

18. The system of claim **16**, wherein the authenticating information comprises a consumer authenticator.

19. The system of claim **16**, wherein the authenticating information comprises a merchant authenticator.

20. The system of claim **11**, wherein the records of the database store other predetermined information in association with the first e-mail address and the second e-mail address, such other information selected from the group comprising a consumer consent, consumer authentication, and merchant authentication.

21. A method for effecting delivery of an e-mail message from a sender to an intended recipient, the intended recipient being associated with a first e-mail address associated with a first Internet service provider (ISP) and a second e-mail address associated with a second ISP, comprising the computer-implemented steps of:

providing an electronic mail address management system (EAMS) database of stored records correlating the first e-mail address of the intended recipient to the second e-mail address of the intended recipient;

at the sender, creating the e-mail message using the intended recipient's first e-mail address;

communicating the e-mail message from the sender to the sender's Internet service provider (ISP) via the Internet;

at the sender's ISP, attempting to deliver the e-mail message to the intended recipient at the first e-mail address;

receiving the e-mail message at the first ISP;

determining at the first ISP that the first e-mail address is not a valid address and generating a "message undeliverable" message in response thereto;

communicating the "message undeliverable" message from the first ISP to the sender's ISP;

in response to receiving the "message undeliverable" message at the sender's ISP, generating a query based on the first e-mail address of the intended recipient;

communicating the query from the sender's ISP to the EAMS database;

in response to the receipt of the query, accessing the EAMS database to determine whether the second e-mail address of the intended recipient is stored in association with the first e-mail address;

in response to a determination that the second e-mail address of the intended recipient is stored in association with the first e-mail address, retrieving the second e-mail address from the EAMS database as a response to the query;

communicating the query response to a computer system not operated by the sender;

modifying the e-mail message to utilize the second e-mail address as the address for the e-mail message; and

automatically transmitting the modified e-mail message to the intended recipient at the second e-mail address without the involvement of the sender.

22. The method of claim **21**, wherein the first ISP is a former ISP associated with the intended recipient and the second ISP is the current ISP associated with the intended recipient.

23. The method of claim **21**, wherein the EAMS database is Internet accessible and the query and query response are communicated via Internet messaging protocols.

24. The method of claim **21**, wherein a computer system associated with the EAMS autoforwards the e-mail message to the second e-mail address in response to receipt of the query response.

25. The method of claim **21**, wherein the query response containing the second e-mail address is provided by the EAMS in response to the query, and wherein a computer system associated with the sender automatically forwards the e-mail message to the second e-mail address in response to receipt of the query response.

26. The method of claim **25**, wherein the sender's ISP autoforwards the e-mail message to the second e-mail address in response to receipt of the query response.

27. The method of claim **21**, further comprising steps for creating a new record in the EAMS database in response to receipt of an address change request from a consumer.

28. The method of claim **27**, further comprising the step of requiring predetermined authenticating information before creating a record in the database.

29. The method of claim **28**, wherein the authenticating information is obtained from an Internet accessible authenticating authority.

30. The method of claim **28**, wherein the authenticating information comprises a consumer authenticator.

31. The method of claim **28**, wherein the authenticating information comprises a merchant authenticator.

32. The method of claim **22**, wherein the EAMS database stores other predetermined information in association with the first e-mail address and the second e-mail address, such other information selected from the group comprising a consumer consent, consumer authentication, and merchant authentication.

33. The system of claim **11**, wherein the process for utilization in automatically re-transmitting the e-mail message to the second e-mail address comprises a program module in said computer system.

34. The system of claim **11**, wherein the process for utilization in automatically re-transmitting the e-mail message to the second e-mail address comprises a program module in a computer system associated with the sender's ISP.

35. A method for managing e-mail address changes, comprising:

providing a database of stored records in a computer system correlating a first e-mail address of an intended recipient of an e-mail message to a second e-mail address of the intended recipient;

in response to a query from a sender's Internet service provider (ISP) associated with the sender of an e-mail message based on the first e-mail address of the intended recipient, accessing the database to determine whether the second e-mail address of the intended recipient is stored in association with the first e-mail address;

in response to a determination that the second e-mail address of the intended recipient is stored in the database in association with the first e-mail address, retrieving the second e-mail address from the database as a response to the query; and

communicating the query response to a process for utilization in automatically re-transmitting the e-mail message to the second e-mail address without the sender's involvement.

36. The method of claim **35**, wherein the first e-mail address is an invalid old address associated with a former Internet service provider (ISP) of the intended recipient and the second e-mail address is a new e-mail address associated with a new ISP of the intended recipient.

37. The method of claim **36**, wherein the query is generated by an Internet service provider (ISP) associated with the sender in response to receipt of a "message undeliverable" message received from the former ISP when the e-mail message was sent to the first e-mail address.

38. The method of claim **35**, wherein the query and query response are communicated via Internet messaging protocols.

39. The method of claim **35**, wherein the process for utilization in automatically re-transmitting the e-mail message to the second e-mail address comprises a program module in a computer system associated with the database.

40. The method of claim **35**, wherein the process for utilization in automatically re-transmitting the e-mail message to the second e-mail address comprises a program module in a computer system associated with the sender's ISP.

41. The method of claim **35**, further comprising the step of creating a new record in the database in response to receipt of an address change request from a consumer.

42. The method of claim **44**, wherein the step of creating the new record in the database includes obtaining predetermined authenticating information before creating a record in the database.

43. The method of claim **42**, wherein the authenticating information is obtained from an Internet accessible authenticating authority.

44. The method of claim **42**, wherein the authenticating information comprises a consumer authenticator.

45. The method of claim **42**, wherein the authenticating information comprises a merchant authenticator.

46. The method of claim **35**, wherein the records of the database store other predetermined information in association with the first e-mail address and the second e-mail address, such other information selected from the group comprising a consumer consent, consumer authentication, and merchant authentication.

* * * * *

US005619648A

United States Patent [19]

Canale et al.

[11] Patent Number: 5,619,648

[45] Date of Patent: Apr. 8, 1997

[54] **MESSAGE FILTERING TECHNIQUES**

[75] Inventors: **Leonard M. Canale**, Tinton Falls; **Henry A. Kautz**, Summit; **Allen E. Milewski**, Red Bank; **Bart Selman**, Summit, all of N.J.

[73] Assignee: **Lucent Technologies Inc.**, Murray Hill, N.J.

[21] Appl. No.: **346,715**

[22] Filed: **Nov. 30, 1994**

[51] **Int. Cl.**[6] **G06F 17/20**

[52] **U.S. Cl.** **395/200.01**; 395/650

[58] **Field of Search** 395/650, 700, 395/200.08, 200.01

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,093,918	3/1992	Heyen et al.	395/200.08
5,377,354	12/1994	Scannell et al.	395/650

OTHER PUBLICATIONS

P. W. Foltz, S. T. Dumais, "Personalized information delivery: An Analysis of Information Filtering Methods", Communications of the ACM, vol. 35, No. 12, Dec. 1992, pp. 51–60.

D.K. Gifford, R. W. Baldwin, S. T. Berlin, J. M. Lucassen, "An Architecture for Large Scale Information Systems", *Proceedings Tenth Symposium on Operating Systems Principles, ACM,* Dec. 1985, pp. 161–170.

E. Lutz, H. V. Kleist-Retzow and K. Hoernig, "MAFIA—An Active Mail-Filter-Agent for an Intelligent Document Processing Support", *Multi-User Interfacws and Applications,* S. Gibbs and A. A. Verrign-Stuart, Eds. North Holland, 1990, pp. 235–251.

T. W. Malone, K. R. Grant, F. A. Turbak, S. A. Brobst, M. D. Cohen, "Intelligent Information-Sharing Systems", *Communications of the ACM,* May 1987, vol. 30, No. 5, pp. 390–402

S. Pollack, "A Rule-Based Message Fultering System", *ACM Trans. on Office Information Systems,* vol. 6, No. 3, Jul. 1988, pp. 232–254.

P. Maes, "Agents that Reduce Work and Information Overload", *Communications of the ACM,* vol. 37, No. 7, Jul. 1994, pp. 31–40.

Primary Examiner—Glenn A. Auve

Attorney, Agent, or Firm—Gordon E. Nelson; David Volejnicek

[57] **ABSTRACT**

Techniques for reducing the amount of junk e-mail received by a user of an e-mail system. A recipient description containing non-address information is added to an e-mail message. The user has an e-mail filter which has access to information which provides a model of the user. The e-mail filter uses the non-address information and the model information to determine whether the e-mail message should be provided to the user. The e-mail filter further has access to information which provides models of the user's correspondents. If the filter does not provide the message to the user, it uses the non-address information and the model information of the user's correspondents to determine who the message might be forwarded to. A sender of e-mail can also use the model information of the sender's correspondents together with the non-address information to determine who the message should be sent to. The techniques are used in a system for locating expertise.

16 Claims, 2 Drawing Sheets

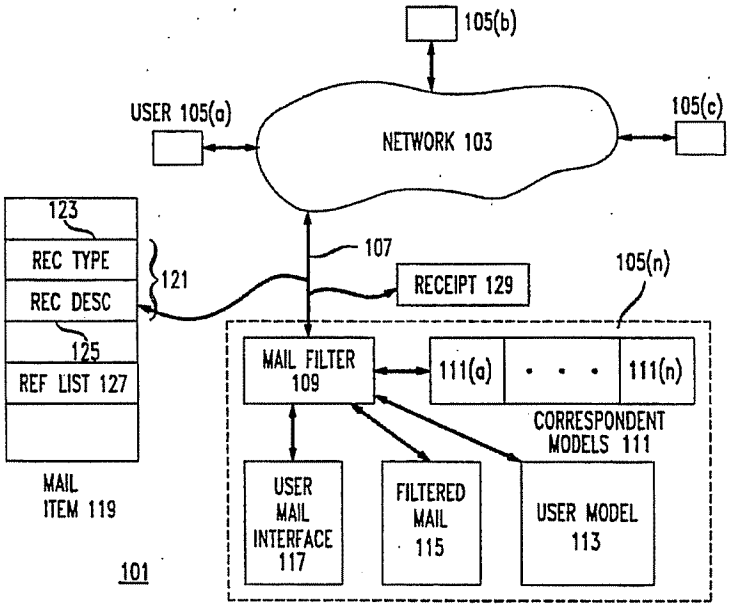


FIG. 1

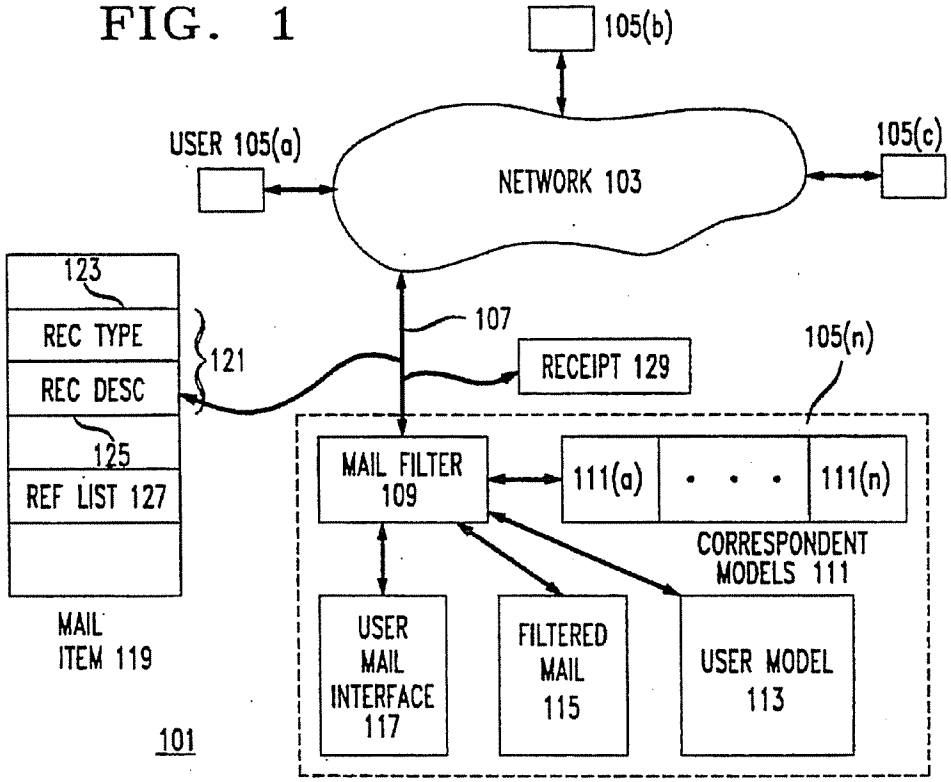

105(b)
USER 105(a)
NETWORK 103
105(c)
123
REC TYPE
REC DESC
121
125
REF LIST 127
MAIL ITEM 119
107
RECEIPT 129
105(n)
MAIL FILTER 109
111(a)
111(n)
CORRESPONDENT MODELS 111
USER MAIL INTERFACE 117
FILTERED MAIL 115
USER MODEL 113
101

FIG. 2

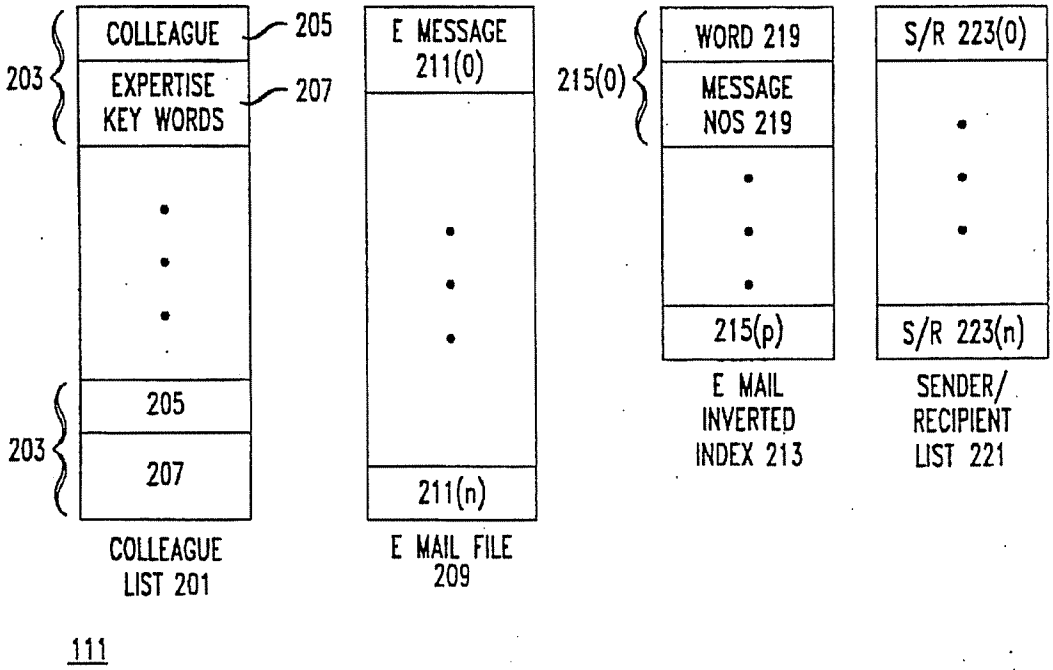

203
COLLEAGUE
205
EXPERTISE KEY WORDS
207
205
207
203
COLLEAGUE LIST 201
E MESSAGE 211(0)
211(n)
E MAIL FILE 209
215(0)
WORD 219
MESSAGE NOS 219
215(p)
E MAIL INVERTED INDEX 213
S/R 223(0)
S/R 223(n)
SENDER/ RECIPIENT LIST 221
111

FIG. 3

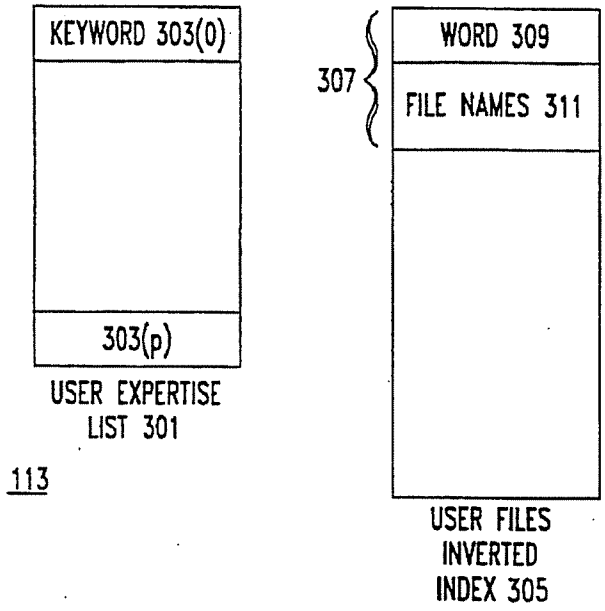
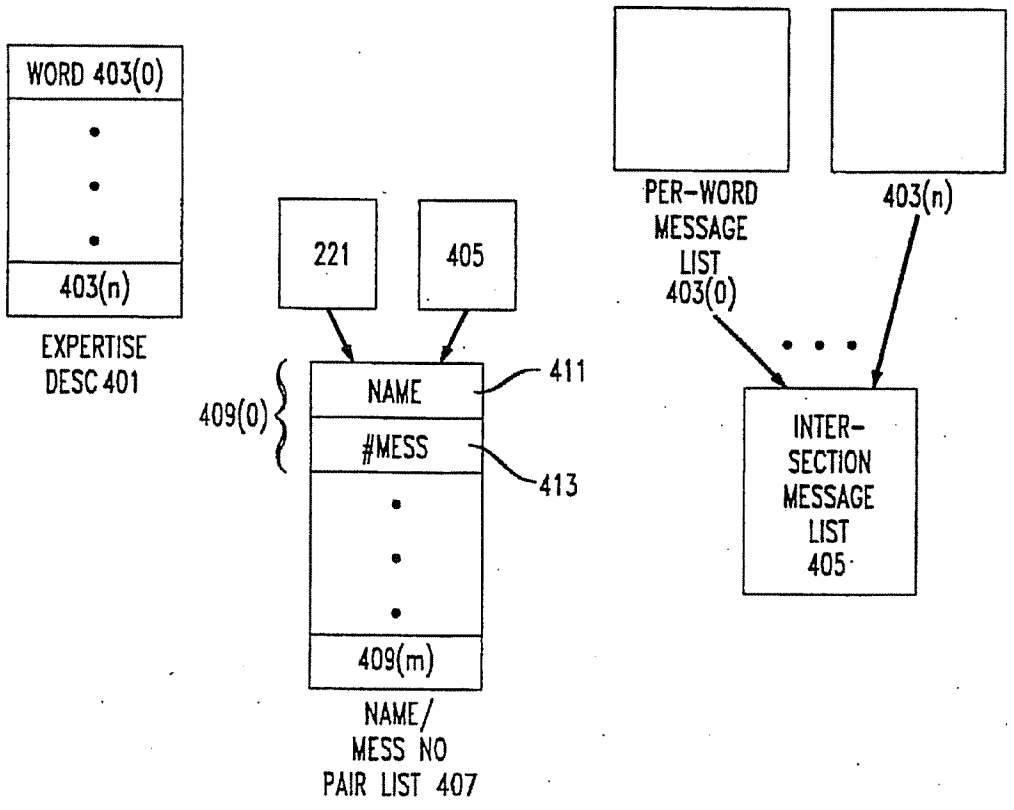

KEYWORD 303(0)
303(p)
USER EXPERTISE LIST 301
113
307
WORD 309
FILE NAMES 311
USER FILES INVERTED INDEX 305

FIG. 4


WORD 403(0)
403(n)
EXPERTISE DESC 401
221
405
409(0)
NAME
#MESS
411
413
409(m)
NAME/ MESS NO PAIR LIST 407
PER-WORD MESSAGE LIST 403(0)
403(n)
INTER-SECTION MESSAGE LIST 405

MESSAGE FILTERING TECHNIQUES

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention concerns electronic messaging in general and electronic mail in particular.

2. Description of the Prior Art

A major annoyance in the conventional mail system is junk mail. As electronic mail has grown in availability and popularity, junk electronic mail has become a problem as well. Indeed, the ease with which an e-mail message may be sent to many recipients may eventually make junk e-mail an even worse problem that junk conventional mail.

The prior art has attempted to deal with the junk e-mail problem by means of mail filters in an e-mail recipient's local e-mail system. Such a filter sorts incoming e-mail for the recipient into categories determined by the recipient. The filter simply scans each e-mail message as it reaches the recipient and determines what category it should be placed in. One category is of course "discard". Messages which the filter places in that category are automatically discarded. Prior-art filters have had varying degrees of intelligence; some have simply worked with lists of source addresses and have sorted according to the source of the message; others have used keywords provided by the recipient to sort; with others, finally, the filter observes how the recipient sorts his e-mail for awhile and is then able to sort in a similar fashion. For details about mail filters, see Peter W. Foltz and Susan T. Dumais, "Personalized information delivery: an analysis of information filtering methods", *Communications of the ACM*, vol. 35, no. 12, Dec., 1992, pp. 51–60; D. K. Gifford, R. W. Baldwin, S. T. Berlin, J. M. Lucassen, "An architecture for large scale information systems", in *Proceedings Tenth Symposium on Operating Systems Principles*, (Orcas Island, Wash., Dec 1985), pp. 161–170; E. Lutz, H. V. Kleist-Retzow, and K. Hoerning, "MAFIA—An active mail-filter agent for an intelligent document processing support", in *Multi-User Interfaces and Applications*, S. Gibbs andn A. A. Verrijn-Stuart, Eds, North Holland, 1990, pp. 16–32; T. W. Malone, K. R. Grant, F. A. Turbak, S. A. Browst, M. D. Cohen, "Intelligent information sharing systems", *Commun. ACM* 30, 5 (May 1987) 390–402; S. Pollack, "A rule-based message filtering system", *ACM Trans. Off. Inf. Syst.* 6, 3 (July 1988), 232–254. P. Maes, "Agents that Reduce Work and Information Overload", *Commun. ACM* 37 (7) (July 1994), pp. 31–40. A problem with all such filters is that sorting for another person is difficult even for a human being, and if a filter is going to be useful, it cannot do much worse than a human would.

One of the reasons for the junk mail is that present-day e-mail systems require that recipients be addressed by e-mail addresses. In order to ensure that an e-mail message will reach everyone who might possibly be interested in it, the sender typically uses a list of addresses which includes those who might be interested but includes many others as well. For everyone but those actually interested, the e-mail is of course junk mail.

What is needed to reduce the amount of junk mail is a technique which permits a sender to use something in addition to the e-mail address to specify the kinds of people who are to actually receive the e-mail and permits a filter to use the information provided by the sender to filter the mail so that only those kinds of people actually receive it. It is an object of the invention disclosed herein to provide such a technique and thereby to reduce the amount of junk e-mail received by a user of the e-mail system.

SUMMARY OF THE INVENTION

The invention reduces the amount of junk e-mail received by a user of the e-mail system by adding a recipient specifier to an e-mail message. The recipient specifier non-address information is used to further specify the recipients in the group to whom the message is sent who should actually receive the message. The mail filter for a given recipient has access to information about that recipient and uses that information together with the non-address information in the e-mail message to determine whether the message should be provided to the given recipient. If the non-address information and the information about the recipient indicate that the given recipient should not receive the message, the filter does not provide it.

In another aspect of the invention, the sender's mail filter does the filtering. The sender provides a recipient specifier which uses non-address information to specify potential recipients to the mail filter. In this aspect, however, the sender's mail filter has access to information about the possible recipients and uses this information together with the non-address information to determine the potential recipients to whom the message should be sent.

The first and second aspects of the invention are combined in a further aspect of the invention, namely a system for locating expertise in the e-mail system. In this system, the sender specifies an area of expertise by means of a list of keywords which are relevant to the area. The list of keywords is included in a recipient specifier in the message. The mail filter for a potential recipient has access to the document files of the potential recipient and to a list of the e-mail messages sent and received by the potential recipient. The mail filter uses the document files to determine the recipient's areas of expertise. If the keywords in the recipient specifier match one of the areas of expertise, the mail filter provides the e-mail message to the potential recipient; if not, the mail filter uses the list of e-mail messages to determine correspondents of the the potential recipient who may have the area of expertise specified in the recipient specifier and forwards the message to those correspondents. The mail filter of each potential recipient which actually provides the message to the recipient further sends a referral message to the sender of the message, who thus knows exactly who received the message.

Other objects and advantages of the apparatus and methods disclosed herein will be apparent to those of ordinary skill in the art upon perusal of the following Drawing and Detailed Description, wherein:

BRIEF DESCRIPTION OF THE DRAWING

FIG. **1** is a high-level block diagram of apparatus embodying the invention;

FIG. **2** is a diagram of user model **113** in a preferred embodiment;

FIG. **3** is a diagram of correspondent models **111** in a preferred embodiment;

and FIG. **4** is a diagram of data structures used by mail filter **109** in a preferred embodiment.

Reference numbers in the Drawing have two parts: the two least-significant digits are the number of an item in a figure; the remaining digits are the number of the figure in

which the item first appears. Thus, an item with the reference number **201** first appears in FIG. **2**.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

The following Detailed Description begins with an overview of the invention and then describes in detail how the invention is implemented in apparatus to locate expertise in an e-mail system.

Overview of the Invention: FIG. 1

FIG. **1** shows a high-level overview of apparatus **101** which embodies the invention. Apparatus **101** is employed in a network **103** which connects a number of users **105**(*a* . . . *n*). Network **103** may be a network such as Internet or a commercial e-mail network, or it may be an e-mail system which communicates between users of a single computer system. Each user **105** is connected to network **103** by means of a link **107** over which user **105** can send and receive e-mail messages. A mail item of the type used in the invention is shown at **119**; mail item **119** is a standard e-mail message except for two additional components:

1. recipient specifier **121** which uses non-address information to further describe the recipients who should receive the e-mail; and

2. referral list **127**, which is a list of potential recipients who passed the e-mail on and of recipients to whom the e-mail was provided.

Recipient specifier **121** has two parts, recipient type field **123**, which generally indicates how recipient specifier **121** is to be interpreted, and recipient description **125**, which contains the non-address information which is actually used to determine whether mail item **119** is to be provided to a given recipient.

A user **105** who wishes to reduce the amount of junk e-mail he receives has a mail filter **109** as part of his e-mail system. When an e-mail item **119** is sent to user **105**'s address, mail filter **109** interprets recipient specifier **121** to determine whether mail item **119** is to be provided to user **105**(*n*). In interpreting recipient specifier **109**, mail filter **109** employs user model **113**, which is data that provides a model of user **105**(*n*). If recipient description **125** specifies a recipient which is of the same kind as that specified by user model **113**, mail filter **109** adds mail item **119** to filtered mail **115** and informs user **105**(*n*) via interactive user mail interface **117** that mail has arrived. If user **105**(*n*) desires, mail filter **109** can further use the information in referral list **127** to indicate the chain of referrals which resulted in the message being directed to user **105**(*n*). In some embodiments, mail filter **109** may also use the information in referral list **127** to send a receipt **129** which identifies the e-mail message, the chain of referrals, and user **105**(*n*) to the original sender of mail item **119**.

If user model **113** does not specify a recipient which is of the same kind specified by recipient description **125**, mail filter **109** looks to correspondent models **111** to determine where to send mail item **119**. There is a correspondent model **111**(*m*) for each of user **105**(*n*)'s frequent correspondents, and like user model **113**, each correspondent model **111**(*m*) contains data which mail filter **109** can use together with recipient description **125** to determine which of user **105**(*n*)'s correspondents should receive mail item **119**. Mail filter **109** then adds the names and e-mail addresses of those correspondents to referral list **127** in mail item **119** and forwards mail item **119** to those correspondents. If they in turn have mail filters **109**, they will also filter mail item **119** as just described. In a preferred embodiment, user **105**(*n*) may specify how much control he desires over forwarding. Forwarding may be completely automatic, or mail filter **109** may present user **105**(*n*) with the information from recipient description **125** and a list of the correspondents it has found for forwarding and let user **105**(*n*) select which of the correspondents is to receive the forwarded letter.

If user **105**(*n*) wishes to send an e-mail message with a recipient specifier **121**, user **105**(*n*) makes that request of mail filter **109**. Mail filter **109** uses interface **117** to obtain information from user **105**(*n*) which it uses to make recipient specifier **121**. Mail filter **109** then uses recipient specifier **121** with correspondent models **111** in the manner described above to make a list of the correspondents who should receive the message. Depending on the implementation, mail filter **109** may simply send the e-mail message to those correspondents or permit user **105**(*n*) to select correspondents from the list. The selected correspondents will of course be placed on referral list **127**. In FIG. **1**, mail filter **109** and correspondent models **111** and user model **113** are all implemented in the local computer system used by user **105**(*n*). Such an implementation is advantageous in that the information in correspondent models **111** and user model **113** remains under the control of user **105**(*n*). In other embodiments, however, mail filter **109** may be located at any point in network **103**. Indeed, some embodiments may contain only correspondent models **111**. For example, a data base of customer information might be used as a correspondent model **111**, and mail filter **109** might use recipient description **125** together with the data base of customer information to determine which customers should receive e-mail about a new product or service.

A System for Locating Expertise

The techniques described above are employed in a preferred embodiment to make a system for locating expertise. The following discussion first explains the utility of such a system and then presents two different embodiments.

Using a Computer to Find Information

There are basically two ways of finding something out by using a computer: "ask a program" and "ask a person".

The first covers all ways of accessing information stored online, including the use of traditional database programs; file indexing and retrieval programs such as glimpse (by Udi Manber at University of Arizona) or Apple's Apple-Search; news filtering programs such as Hoover (SandPoint Corp.); and even more simply, the use of tools such as ftp, awk, and text editors to retrieve and view files.

The second, "ask a person", covers ways that a computer can be used as a communication medium between people. Currently the prime examples are electronic mail, including both personal e-mail and mailing lists, and bulletin boards and newsgroups. The growing integration of computers and telephones allows us to also view telephony as a computer-based communication medium. Simple examples of such integration are telephone address book programs that run on a personal or pocket computer and dial numbers for you; more sophisticated is the explosion in the use of computer-based FAX. Today it is hard to even buy a modem that does not have FAX capability, and by far the heaviest use of FAX is for person-to-person communication.

There are inherent problems with both general approaches to obtaining information. It has often been noted that as the world of online information sources expands, the "ask a program" approach suffers from the problem of knowing where to look. For example, the Mosaic system overcomes many of the technical problems in accessing a wide variety of information on the Internet, by automatically handling the low-level details of different communication protocols. It is easy and entertaining to browse through an enormous hypermedia space. However, finding an answer to a specific question using Mosaic tends to be slow and frustrating, and often results in failure. One response to this problem has been the attempt to design systems that incorporate knowledge about the location of information, such as the Information Manifold project (by T. Kirk, A. Levy, and D. Srivastava, of AT&T Bell Labs). However, a deeper problem remains, that no solution based solely on building a better search-engine can address. This is the fact that much valuable information is simply not online, but only exists in people's heads. Furthermore, there are economic, social, and political reasons that much valuable information will never be made publicly accessible on the Internet or any other network. Indeed, part of the value of a piece of information resides in the degree to which it is not easily accessible.

In any large organization, determining who is an expert on a particular topic is a crucial problem. The need for expertise location ranges from informal situations, such as where I might need to find an expert on LaTex macros to help fix a typesetting problem in a paper I'm writing, to formal construction of project teams to meet business needs. The range of expertise specifications may range from the generic ("who knows about logic programming?") to the highly specific ("who knows how to modify the interrupt vector handling microcode in the reboot module of the XZY999 processor?").

Online directories of expertise rarely exist, and when they do, the information that contain is certain to be out of date and incomplete. In fact, expertise needs are potentially so specific that it is simply impossible to determine a comprehensive set of categories in advance. Expertise location is therefore generally an "ask a person" task, with the all the problems associated with that approach outlined above.

Let us consider for a moment how expertise location actually works when it is successful. In a typical case I contact a small set of colleagues whom I think might be familiar with the topic. Because each person knows me personally, they are quite likely to respond. Usually none of them is exactly the person I want; however, they can refer me to someone they know who might be. After following a chain of referrals a few layers deep I finally find the person I want.

Note that in this successful scenario I needed to walk a fine line between contacting too few people (and thus not finding the true expert) and contacting too many (and eventually making a pest of myself). Even in the end I might wonder if I might not have found even a better expert if only I could have cast the net a bit wider. I may have had difficulty bringing to mind those people I do know personally who have some expertise in the desired area. If only all of my colleagues employed endlessly patient assistants that I could have contacted initially, who would have known something about their bosses' areas of expertise, and who could have answered my initial queries without disturbing everyone.

Now let us consider how mail filters could be used to augment the expert location process. Each person's mail filter would create a model of that person's areas of interest. This model would be created automatically by using information retrieval (IR) techniques (such as inverted indexes) on all the documents created and received by the user. The user model could be quite large and detailed, and would be private to the user, that is, not stored in a central database. The mail filter would also create a much more coarse-grained model of my contacts by applying similar techniques to all the electronic mail that I exchange with each person.

When I have an expertise location need, I present the problem to my mail filter as an unstructured text description. Again using IR techniques, my mail filter selects a medium-to-large set of my contacts to whom the query may be relevant. It then broadcasts the query, not to the people themselves, but to their mail filters. Upon receipt of the question, each mail filter checks if its owner's user model does indeed provide a good match. If there is a good match, the mail filter presents my request to its owner. If the owner's model does not match, but the model of one of the owner's contacts does, then the mail filter can ask the owner if it can provide a referral. Finally, if there is no match at all, the query is silently logged and deleted. A great deal of flexibility can be built into each mail filter, depending upon its owner's preferences. For example, I might allow automatic referrals to be given to requests that come from my closest colleagues.

This system provides several benefits over either sending personal e-mail to everyone in order to find an expert or using netnews to find the expert. First, it is largely passive on the part of the recipients—they do not need to be reading netnews and wading through dozens of articles. Second, queries are broadcast in a focused manner to those who are at least somewhat likely to find them of interest. Third, users are shielded from seeing a large number of completely irrelevant messages; each mail filter **109** may process dozens of messages for every one the user sees. Finally, messages that a user does see do not come from "out of the blue", but rather are tagged with a chain of referrals from colleague to colleague.

One reason to believe that the system just described would be useful in practice is that it basically models the manner in which expertise location actually works now (D. Krackhardt and J. R. Hanson, "Informal Networks: The Company Behind the Chart", Harvard Business Review, July-August 1993), while allowing more people to be contacted without causing disruption and disturbance.

Implementation of an Expertise Locator

A presently-preferred embodiment of the expertise locator has been implemented using the network agents described in Coen, et al., *Network Agents,* U.S. patent application Ser. No. 08/203,147, filed Feb. 28, 1994 abandoned and continued as U.S. Ser. No. 08/513,417, filed Aug. 10, 1995. In the implementation, mail filter **109** is a component of a user agent which handles e-mail messages for its user. Mail filters **109** are written in the programming language Visual Basic, and run on a standard personal computer. Interactive user mail interface **117** presents the expertise locator in mail filter **109** to the user as an anthropomorphic "talking head" that appears in a window on the computer screen. All the computers running mail filters **109** are networked (currently using the protocol TCP/IP), and can exchange electronic mail with each other and with any person. A mail filter **109** can also invoke other programs to perform various subtasks.

Each mail filter **109** has access to two sets of data base files. The first set, shown in FIG. **2**, implements correspon-

dent models **111**; the second set, shown in FIG. **3**, implements user model **113**. Each of the data base files in the two sets is specific to and owned by the individual user of mail filter **109**. It is important to note that we do not assume that these files can be directly accessed by anyone other than the user and mail filter **109**.

Correspondent models **111** contains the following five files:

Colleague list **201** which contains entries **203** for some of the user's colleagues. Each entry **203** contains an identification **205** for the colleague and each a list of keywords **207** describing the colleague's areas of expertise.

An Email file **209** which contains all of the email **211**(**0**..*n*) that the user has sent and received for a substantial period of time: typically, the past year or several years.

An Email inverted index file **213** that has an entry **215** for each word that appears in any email message. Entry **215** contains a word **217** and a list of the numbers of the messages in email file **209** that contain that word. This kind of file can be generated using standard information retrieval algorithms, such as those described in (G. Salton, *Automatic Text Processing*, Addison-Wesley 1989).

A sender/recipient list file **221** that has an entry **223** for each message in email file **209**. The entry contains the identifier of the sender of the corresponding message (if other than the user) or the identifier of the recipient of the corresponding message (if sent by the user).

FIG. **3** shows the data base files used to implement user model **113**.

User expertise list **301** is a file containing a list of keywords that describe some of the user's own areas of expertise.

User files inverted index **305** is a file containing an inverted index of text files in the user's directory. That is, for every word that appears in any file the user has stored on the computer, this file contains a list of the names of the files containing that word.

In the preferred embodiment, colleague list **201** and user expertise list **301** are created by mail filter **109** in interaction with user **105**(*n*); the inverted index files **213** and user files inverted index **305** are created automatically by mail filter **109**. This kind of very large inverted index can be quickly created and searched by the program "glimpse" (U. Manber and S. Wu, "GLIMPSE: A Tool to Search Through Entire File Systems," *Usenix Winter* 1994 *Technical Conference*, San Francisco (January 1994), pp. 23–32). In making inverted list **305**, GLIMPSE uses a UNIX operating system (UNIX is a trademark of XOPEN) utility which determines whether a file is a text file. In addition, the user can specify to GLIMPSE which directories of files or individual files are to be indexed.

A user begins the process of locating an expert in a topic by clicking on the window for mail filter **109** and typing a phrase that describes the general kind of request (such as, "I need to locate an expert"). Mail filter **109** then prompts the user for a phrase describing the area of expertise. Once this is done, mail filter **109** generates and presents for approval a list of suggested candidates for receiving the request.

The list of candidates is generated by combining names from two sources. First, names are added that appear in colleague list **201**, such that the words that appear in the phrase describing the expertise request appear in the list of keywords **207** associated with name **205**.

Second, names are added that result from the following computation. First, for each word that appears in the expertise request, mail filter **109** retrieves from email inverted index file **213** a list of messages **403**(**0** . . . n) (FIG. **4**) containing that word. Next, the intersection of the lists is computed, generating a list of messages **405** each of which appears in every one of the previous lists. Next, list of messages **405** is compared against sender/recipient list file **221**, and the total number of messages that appear in list of messages **405** that are from each person in sender/recipient list **221** is calculated. The result is a name/message number pair list **407** of pairs of "person name" and "number of messages". Finally, list **407** is sorted according to "number of messages". The 20 names with the highest number of messages in this list are then added to the list of candidates.

After the list of candidates has been approved by the user, mail filter **109** makes a recipient specifier **121** and adds it to the email message. Recipient specifier **121** contains a recipient type request **123** which specifies that an expert is being requested and expertise description **401** is used as recipient description **125**.

The message travels through the network and arrives at the computer systems(s) of the recipients. Each recipient mail filter **109** notes recipient specifier **121** specifying that an expert is being requested, removes the e-mail message from the incoming mail stream, and processes it as follows:

First, the words in expertise description **401** contained in the message's recipient specifier **121** are matched against the recipient's user expertise list **301**. If the words appear in list **301**, then mail filter **109** assumes that this request is appropriate for the recipient to see.

If the words in the phrase do not match against the contents of user expertise list **301**, mail filter **109** uses user files inverted index file **305** to match the phrase against the contents of all of the recipient's files which are indexed in file **305**. This matching can be efficiently performed using the program "GLIMPSE" mentioned above. If the number of matches is greater then a threshold number (e.g., more than 10 matches), the recipient's mail filter **109** determines that this request is likely to be appropriate for the recipient.

If the recipient's mail filter thus determines in either way that the message is appropriate, it uses user mail interface **117** to make the the message appear on the recipient's computer screen. The recipient is then given the option of (i) responding affirmatively back to the sender; (ii) responding negatively back to the sender; or (iii) referring the request to someone else. If this final option is selected, the recipient's mail filter **109** creates a list of candidate recipients as described above and the process is repeated.

As is apparent from the foregoing description, the preferred embodiment of the expertise locator increases its efficiency by using two-stage correspondent models **111** and user models **113**. The first stage is the explicit descriptions of expertise contained in colleague list **201** and user expertise list **301**; the second stage is the inverted indexes: inverted index **213** into email file **209** and inverted index **305** into the the user's text files. The algorithms first use the expertise lists **201** and **301**, and then they may in addition use the inverted indexes.

EXAMPLE II

Enhanced Yellow Page Service

The general techniques described above can be applied to many different kinds of tasks. The general approach is useful when the following conditions hold:

1. You wish to contact a large number of people, without necessarily broadcasting messages to everyone in the world. In the expertise location example, the user agent helped

determine a preliminary list of candidates based on a matching scheme. Other ways of determining whom to send the message to are also useful. In the example below, the recipients are simply taken to be a fixed list of the sender's friends and colleagues.

2. You want the message you send to only be seen by people to whom is it very likely to relevant, in order to avoid being disruptive. To that end,you want the message you send to explicitly indicate the conditions under which which it should be taken to be relevant. Note that the computation of relevancy may rely on information that is private to the recipient. In the previous example, the sender indicated the general conditions of relevancy by recipient type field **123** (thus indicating the general kind of processing to be performed by the recipient's mail filter **109**) and the words in recipient description field **125** describing the kind of expertise required (thus providing the parameters to that processing). Another way of saying this is that the sender proactively determines the general manner in which the message is to be em filtered. Note that this is different from earlier work on mail filtering, which always assumes that the recipient of a message is completely responsible for establishing the conditions for filtering (if any), and the sender is completely "passive" with regard to filtering.

We illustrate these core points with the following "Enhanced Yellow Page" service. The basic idea is to provide a service that assists people in obtaining one or more personal recommendations about a professional service or business. The system would work as follows.

A customer contacts the Enhanced Yellow Page Service (EYPS) asking for a number of a particular service (e.g., a flower delivery service, an autobody shop, a roofer, etc.). The contact with the EYPS could be made by many possible means of communication, including telephone, an on-line service, an internet Mosaic/HTTP server, or electronic mail; alternatively, the EYPS software and directory could even be distributed to users and run entirely on their personal computers.

The EYPS gives one or more possible numbers. The customer can then ask the EYPS to help in obtaining one or more personal recommendations about the service or business.

To obtain the recommendations, the EYPS first considers people from a list of friends or colleagues of the customer. (One way to obtain this list is by simply asking the customer to register friends, family, or colleagues but there are also less intrusive ways of doing this, such as by keeping track of people with whom the customer frequently communicates.)

Now, the key idea is that the EYPS does not simply contact every person on the list, but rather only contacts those people that have dealt with the particular service or business number in the last couple of months. There are at least two ways in which this kind of "sender pro-active filtering" can be done:

1. The EYPS contacts mail filter **109** for each friend or colleague, indicating the name and telephone number for the service for which a recommendation is desired. Mail filters **109** that have been trusted with their owner's telephone records and/or records of business transactions can determine whether their owner has dealt with that company. If so, they pass the request on to the owner.

2. If the EYPS has direct access to the telephone records of the friends and colleagues (which is the case if the EYPS is implemented by a program running in a long-distance network itself), then it checks the phone records itself to determine the list friends and colleagues that have called that company.

Thus, instead bothering a large group of people, there is a careful screening to ensure that only those are contacted who have had some recent dealings with the particular service or business. There are various ways of how the EYPS can complete the process. The least intrusive way would be to simply leave a message with some of the selected people saying "Mr. or Ms. X would be interested in any opinion or recommendation about service Y. Please contact X at or leave message at number Z. This request expires at midnight".

Note that this kind of "pro-active" mail filtering can also be implemented by having the user send a message directly to someone's mail filter **109**. The message header would include a directive saying "pass on to user if he or she has contacted service X at least twice in the last three months." Upon receipt of the message, mail filter **109** will now filter the message based on the included directive. Again, note the difference with the current forms of mail-filtering, where filtering is under complete control of the recipient, and the sender does not give direct instructions to the filtering program.

Such a system naturally raises many privacy issues that can be addressed. For example, you may not necessarily let the person seeking the recommendation know who gets the request-for-advice message. That way, people would not feel obliged to respond. Also, the identify of the requester could be protected by simply having a message saying "A friend would like an opinion or recommendation about service Y." In that case the EYPS would only reveal the identity of the requester once the recipient agrees to respond.

Conclusion

The foregoing Detailed Description has disclosed to those skilled in the computer and networking arts how non-address recipient information in an e-mail message and a mail filter which includes a model of the recipient may be used to reduce the amount of junk e-mail received by the recipient and how the non-address recipient information and a mail filter which includes models of the sender's correspondents may be used to reduce the amount of e-mail sent by a user. The Detailed Description has further disclosed how the above techniques may be used to construct an expertise locator and has disclosed the best mode presently known to the inventors for implementing the expertise locator.

It will be immediately apparent to those skilled in the computer and networking arts that the principles of the invention may be used in any situation where a mail filter has access to information which enables it to respond to non-address information about the potential recipients of an e-mail message. It will be further apparent that many techniques may be used to construct models of the correspondents and recipients for use by the mail filters. The models may be simple lists of keywords, they may be inverted files, they may be data bases, or they may be any other arrangement of data which permits the mail filter to determine from the model and the non-address information whether the potential recipient should actually receive the message. It will further be apparent to those skilled in the art that the location of the mail filter in the network is a matter of design choice. Filters which are located on the same computer system as the recipient have better access to recipient information, while those which are located closer to the

sender are more efficient at reducing the total amount of network traffic.

All of the above being the case, the foregoing Detailed Description is to be understood as being in every respect illustrative and exemplary, but not restrictive, and the scope of the invention disclosed herein is not to be determined from the Detailed Description, but rather from the claims as interpreted according to the full breadth permitted by the law.

What is claimed is:

1. Apparatus for automatically limiting the recipients of a message sent via a mail system implemented in a computer system, the apparatus comprising:

recipient specifying means in the message which uses non-address information to specify the recipients of the message;

message filtering means in the computer system having access to recipient information contained therein about at least one potential recipient and including means responsive to the non-address information and to the recipient information for providing the message to the at least one potential recipient if the non-address information and the recipient information together indicate that the at least one potential recipient is to receive the message; and

means, in the message filtering means, for sending a referral message to a source of the message when the message filtering means provides the message to the at least one potential recipient.

2. The apparatus set forth in claim **1** wherein:

the referral message contains an identification of the at least one potential receipient.

3. The apparatus set forth in claim **1** wherein:

the message is received by a plurality of users;

the message includes information specifying the users who received the message; and

the referral message further contains the information specifying the users who received the message.

4. An arrangement for locating expertise in a messaging system implemented in a computer system, comprising:

first means, included in a message, for indicating, via non-address information, expertise sought by a sender of the message;

second means in the computer system, for determining expertise of an addressee of the message;

third means in the computer system responsive to receipt of the message, for determining whether the expertise indicated by the first means matches the expertise of the addressee determined by the second means;

fourth means in the computer system responsive to a determination by the third means that the indicated expertise matches the determined expertise, for providing the message to the addressee, and responsive to a determination by the. third means that the indicated expertise does not match the determined expertise, for preventing the message from being provided to the addressee;

fifth means in the computer system, for determining expertise of contacts of the addressee;

sixth means responsive to a determination that the indicated expertise does not match the determined expertise of the addressee, for determining whether the indicated expertise matches the expertise of any said contacts determined by the fifth means; and

seventh means responsive to a determination by the sixth means that the indicated expertise matches the determined expertise of a contact, for sending the message to that contact.

5. The arrangement of claim **4** wherein:

the second, third, and fourth means are associated with the addressee.

6. The arrangement of claim **4** wherein:

the fifth and sixth means are associated with the addressee.

7. The arrangement of claim **4** further comprising:

eighth means responsive to a determination by the sixth means that the indicated expertise does not match the determined expertise of any contact, for discarding the message.

8. The arrangement of claim **7** wherein:

the eighth means are associated with the addressee.

9. The arrangement of claim **4** wherein:

the fifth means comprise

means for analyzing messages exchanged by the sender with the contacts to determine therefrom the expertise of the contacts.

10. The arrangement of claim **4** further comprising:

eighth means in the computer system responsive to the sixth means determining that the indicated expertise matches the determined expertise of a contact, for including referral information in the message to indicate that the message is being sent from the addressee to that contact.

11. The arrangement of claim **4** wherein:

the first means comprise

means for conveying a list of keywords.

12. An arrangement for locating expertise in a messaging system implemented in a computer system, comprising:

first means, included in a message, for indicating, via non-address information, expertise sought by a sender of the message;

second means in the computer system, for analyzing files of an addressess of the message to determine therefrom expertise of the addressee;

third means in the computer system responsive to receipt of the message, for determining whether the expertise indicated by the first means matches the expertise of the addressee determined by the second means; and

fourth means in the computer system responsive to a determination by the third means that the indicated expertise matches the determined expertise, for providing the message to the addressee, and responsive to a determination by the third means that the indicated expertise does not match the determined expertise, for preventing the message from being provided to the addressee.

13. An arrangement for locating expertise in a messaging system implemented in a computer system, comprising:

first means, included in a message, for indicating, via non-address information, expertise sought by a sender of the message;

second means in the computer system, for determining expertise of an addressee of the message;

third means in the computer system responsive to receipt of the message, for determining whether the expertise indicated by the first means matches the expertise of the addressee determined by the second means;

fourth means is in the computer system responsive to a determination by the third means that the indicated expertise matches the determined expertise, for provid-

ing the message to the addressee, and responsive to a determination by the third means that the indicated expertise does not match the determined expertise, for preventing the message from being provided to the addressee;

fifth means in the computer system for analyzing messages exchanged by the sender with potential recipients of the message to determine therefrom the expertise of the potential recipients; and

sixth means in the computer system responsive to generation of the message by the sender, for selecting addressees of the message from the potential recipients by matching the expertise sought by the sender with the expertise of the potential recipients determined by the fifth means.

14. The arrangement of claim **13** further comprising:

messaging means for sending the message to the selected addressees of the message.

15. The arrangement of claim **13** wherein:

the fifth and sixth means are associated with the sender.

16. An arrangement for locating expertise in a messaging system implemented in a computer system, comprising:

first means, included in a message, for indicating, via non-address information, expertise sought by a sender of the message;

second means in the computer system, for determining expertise of an addressee of the message;

third means in the computer system responsive to receipt of the message, for determining whether the expertise indicated by the first means matches the expertise of the addressee determined by the second means;

fourth means in the computer system responsive to a determination by the third means that the indicated expertise matches the determined expertise, for providing the message to the addressee, and responsive to a determination by the third means that the indicated expertise does not match the determined expertise, for preventing the message from being provided to the addressee; and

fifth means in the computer system responsive to the fourth means providing the message to the addressee, for sending a referral message to the sender to inform the sender that the message was provided to the addressee.

* * * * *

(X) RELATED PROCEEDINGS APPENDIX

None.